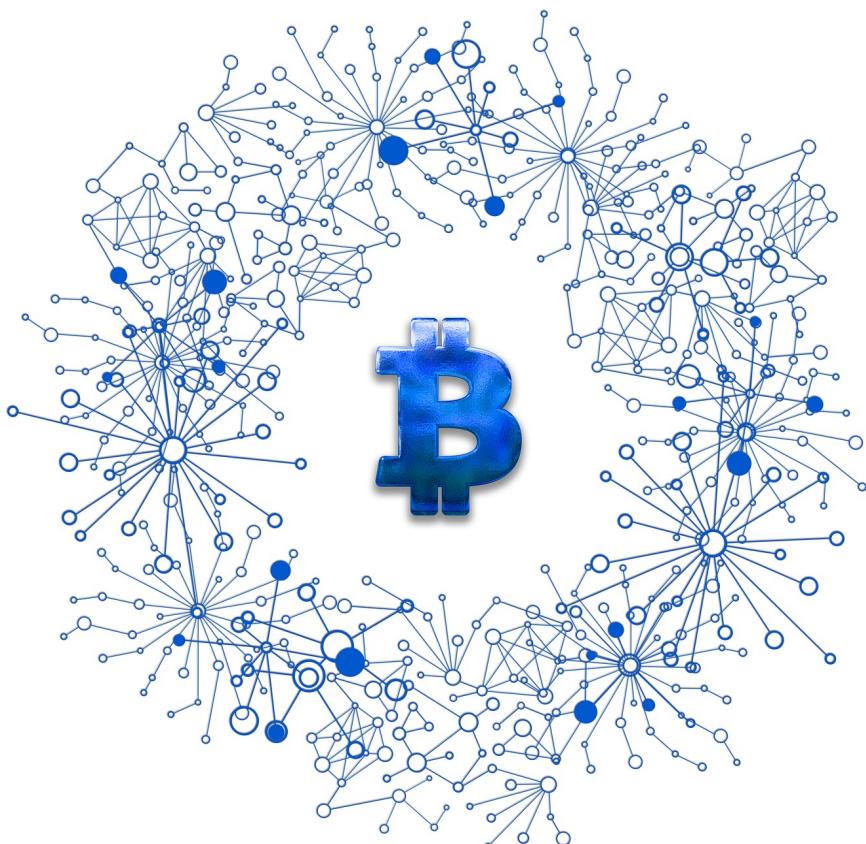


DCA Master



Membri del team:
Adriano Donati - 0000889135
Giovanni Taddei - 0000874948
Jacopo Tamagnini - 0000880252

Indice

| | |
|--|-----------|
| Analisi dei Requisiti e del Rischio | 7 |
| Raccolta dei requisiti | 7 |
| Tabella dei requisiti | 8 |
| Analisi del Dominio | 10 |
| Vocabolario | 10 |
| Sistemi Esterne | 12 |
| Analisi dominio applicativo | 12 |
| Analisi Requisiti | 13 |
| Modello dei Casi d'Uso | 13 |
| Scenari | 14 |
| Registrazione | 14 |
| AggiornaValori | 15 |
| ResocontoMensile | 15 |
| Autenticazione | 16 |
| VisualizzaAndamento | 17 |
| FiltroVisualizzazione | 18 |
| SceltaParametri | 19 |
| ConfigurazionePortafoglio | 20 |
| RimozioneAccount | 20 |
| AttuazioneInvestimento | 21 |
| VisualizzaUtente | 22 |
| Analisi del rischio | 23 |
| Valutazione dei beni | 23 |
| Tabella minacce/controlli | 24 |
| Analisi delle tecnologie della sicurezza | 25 |
| Security Use Case e Misuse Case | 26 |
| Modello | 26 |
| Scenari | 27 |
| SicurezzaComunicazioni | 27 |
| GarantireProtezione | 28 |
| ControlloAccesso | 29 |
| Requisiti di sicurezza | 30 |
| Analisi del problema | 31 |
| Analisi delle Funzionalità | 31 |
| Tabella delle Funzionalità | 31 |
| VisualizzaAndamento: Tabella Informazioni/Flusso | 32 |
| SceltaParametri: Tabella Informazioni/Flusso | 32 |
| ConfigurazionePortafoglio: Tabella Informazioni/Flusso | 32 |
| Registrazione: Tabella Informazioni/Flusso | 33 |

| | |
|---|----|
| Autenticazione: Tabella Informazioni/Flusso | 33 |
| RimozioneAccount: Tabella Informazioni/Flusso | 33 |
| ResocontoMensile: Tabella Informazioni/Flusso | 34 |
| AttuazioneInvestimento: Tabella Informazioni/Flusso | 34 |
| AggiornaValori: Tabella Informazioni/Flusso | 35 |
| VisualizzaUtente: Tabella Informazioni/Flusso | 35 |
| CreazioneLog: Tabella Informazioni/Flusso | 35 |
| AnalisiLog: Tabella Informazioni/Flusso | 36 |
| VisualizzaLog: Tabella Informazioni/Flusso | 36 |
| Analisi dei vincoli | 37 |
| Tabella vincoli | 37 |
| Analisi delle interazioni | 38 |
| Tabella maschere | 38 |
| Tabella sistemi esterni | 39 |
| Analisi Ruoli e Responsabilità | 40 |
| Tabella Ruoli | 40 |
| Utente: Tabella Ruolo-Informazioni | 41 |
| Amministratore: Tabella Ruolo-Informazioni | 42 |
| Scomposizione del Problema | 43 |
| Tabella scomposizione funzionalità | 43 |
| Registrazione: Tabella Sotto-Funzionalità | 43 |
| AttuazioneInvestimento: Tabella Sotto-Funzionalità | 43 |
| Modello del dominio | 44 |
| Architettura logica: struttura | 46 |
| Diagramma dei package | 46 |
| Diagramma delle classi: Dominio | 46 |
| Diagramma delle classi: Controller & Interfacce | 47 |
| AggiornaValori & InterfacciaAggiornaValori | 47 |
| RimuoviUtente & InterfacciaRimozioneUtente | 47 |
| CreazioneResoconto & InterfacciaEmail | 47 |
| VisualizzazioneAndamento & InterfacciaVisualizzazioneAndamento | 48 |
| GestioneDCA & InterfacciaGestioneDCA | 49 |
| Autenticazione & InterfacciaAutenticazione | 49 |
| Registrazione & InterfacciaRegistrazione & InterfacciaEmail | 50 |
| VisualizzazioneUtente & InterfacciaVisualizzazioneUtente | 50 |
| Log & InterfacciaLog | 51 |
| AttuazioneInvestimento & InterfacciaAttuazioneInvestimento & InterfacciaEmail | 51 |
| Architettura logica: interazione | 52 |
| Diagrammi di sequenza | 52 |
| Registrazione | 52 |

| | |
|--|-----------|
| Autenticazione | 53 |
| AttuazioneInvestimento | 54 |
| Diagrammi di Stato/Attività | 55 |
| Piano di lavoro | 56 |
| Sviluppi Futuri | 57 |
| Piano del collaudo | 58 |
| Progettazione | 60 |
| Progettazione architetturale | 60 |
| Requisiti non funzionali | 60 |
| Scelta dell'architettura | 61 |
| Scelte tecnologiche | 61 |
| Progettazione di dettaglio: Struttura | 65 |
| Diagramma di dettaglio: Dominio | 65 |
| Gestione Investimenti e Strategia DCA | 65 |
| Gestione Utente, Amministratore e Valuta Fiat di Riferimento | 66 |
| Gestione Aggiornamento Valori Criptovalute | 66 |
| Gestione Log | 67 |
| Diagramma di dettaglio: Interfacce nei server | 68 |
| Diagramma di dettaglio: Controller | 69 |
| Gestione Utente | 69 |
| AttuazioneInvestimento | 70 |
| VisualizzazioneAndamento | 71 |
| GestioneDCA | 72 |
| AggiornaValori | 73 |
| CreazioneResoconto | 73 |
| Log | 74 |
| Diagramma di dettaglio: Broker | 74 |
| Diagramma di dettaglio: Client | 75 |
| Utente | 75 |
| Interfaccia Registrazione | 76 |
| Interfaccia Login | 77 |
| Interfaccia RimozioneAccount | 77 |
| Interfaccia VisualizzazioneAndamento | 78 |
| Amministratore | 79 |
| Diagramma di dettaglio: Interazione | 80 |
| Registrazione | 80 |
| Autenticazione | 81 |
| AttuazioneInvestimento | 82 |
| Diagramma di dettaglio: Comportamento | 82 |
| Progettazione della persistenza | 83 |
| Diagramma ER | 83 |

| | |
|------------------------------|----|
| Formato del File Log | 84 |
| Progettazione del collaudo | 85 |
| Progettazione del deployment | 88 |
| Deployment per la sicurezza | 88 |
| Deployment del sistema | 89 |

Abstract

L'obiettivo del progetto è creare uno strumento che permetta di automatizzare gli investimenti sulle criptovalute, tramite la tecnica del DCA(dollar cost averaging).

Il programma avrà un'interfaccia verso le API offerte da una piattaforma di exchange per poter effettuare gli acquisti delle criptovalute, la chiave API andrà protetta tramite crittografia.

Il pagamento automatico ricorrente da parte degli utenti verrà offerto mediante l'utilizzo di servizi di membership offerte da portafogli online (es. Paypal).

Sarà possibile consultare lo storico delle transazioni avvenute ed i prezzi in tempo reale delle rispettive valute, utilizzati poi per calcolare l'andamento nel tempo del portafoglio e tracciare grafici all'interno dell'interfaccia utente.

Analisi dei Requisiti e del Rischio

Raccolta dei requisiti

1. L'utente deve poter analizzare l'andamento del valore del proprio portafoglio su un'interfaccia grafica
2. Il sistema attua la strategia del Dollar Cost Averaging, facendo scegliere all'utente una frequenza temporale e una percentuale, sulla spesa totale, che vuole investire per ogni criptovaluta
3. La distribuzione percentuale delle criptovalute deve poter essere modificata in qualsiasi momento
4. Per accedere al sistema l'utente deve autenticarsi con delle credenziali scelte in fase di registrazione
5. Il sistema calcola una previsione della spesa dell'utente
6. Il sistema può gestire autonomamente il deposito di valuta fiat sul portafoglio di criptovalute
7. E' possibile visualizzare e filtrare in base a moneta, spesa e intervallo di date la cronologia degli acquisti e l'andamento del portafoglio
8. L'amministratore può analizzare tutti gli investimenti previa autenticazione con credenziali
9. Al termine di ogni mese all'utente viene inviato un resoconto del mese appena trascorso con un riepilogo dell'evoluzione del proprio portafoglio
10. L'utente deve poter richiedere la terminazione dell'iscrizione al servizio.

Punti emersi in seguito ad una successiva analisi dei requisiti raccolti:

11. L'utente deve scegliere una valuta fiat di riferimento che sarà usata per effettuare le analisi delle variazioni del portafoglio
12. L'utente deve impostare un metodo di pagamento usato per effettuare i depositi e gli investimenti
13. Le informazioni relative al valore delle criptovalute devono essere aggiornate ogni 30 secondi

Tabella dei requisiti

| ID | Requisito | Tipo |
|------|--|------------|
| R1F | Acquisto automatico, ogni intervallo di investimento scelto dall'utente, di criptovaluta dalla piattaforma di exchange e salvataggio sul sistema del riepilogo dell'ordine | Funzionale |
| R2F | Aggiornamento, ogni 30 secondi, del valore attuale delle criptovalute | Funzionale |
| R3F | Recupero e calcolo del valore in valuta fiat per il portafoglio di ogni utente | Funzionale |
| R4F | L'utente sceglie un intervallo di investimento in giorni e un budget totale, che non possono essere negativi o nulli | Funzionale |
| R5F | L'utente sceglie un insieme di criptovalute e la percentuale del budget che ciascuna occupa, che può essere modificata in qualsiasi momento | Funzionale |
| R6F | L'utente deve registrarsi al sistema inserendo l'indirizzo di posta elettronica, uno username, una password, una valuta fiat di riferimento e un metodo di pagamento. L'email dovrà essere verificata attraverso un codice di verifica | Funzionale |
| R7F | Il sistema calcola una previsione della spesa totale futura dell'utente per i prossimi 12 mesi | Funzionale |
| R8F | Il sistema gestisce il deposito di valuta fiat sul portafoglio dell'utente | Funzionale |
| R9F | L'utente può visualizzare lo storico delle transazioni, che può essere filtrato in base a moneta, spesa e intervallo di date | Funzionale |
| R10F | L'amministratore può visualizzare i riepiloghi degli ordini degli utenti | Funzionale |
| R11F | Ogni mese all'utente viene inviato, via posta elettronica, un resoconto relativo all'andamento del portafoglio | Funzionale |
| R12F | Nel resoconto mensile sono riportati: la variazione del valore del portafoglio rispetto all'inizio del mese, la spesa totale complessiva mensile e la spesa per ogni moneta | Funzionale |
| R13F | L'utente può richiedere la terminazione della sua iscrizione al servizio | Funzionale |
| R14F | Il sistema traccia dei grafici che mostrano l'andamento del valore del portafoglio dell'utente, filtrabile per moneta, | Funzionale |

| | | |
|------|--|----------------|
| | spesa e intervallo di date | |
| R15F | Il sistema mostra all'utente una lista delle criptovalute acquistabili per la sua valuta di riferimento | Funzionale |
| R16F | L'utente per usufruire dei servizi del sistema deve effettuare l'accesso con il suo username e password | Funzionale |
| R17F | Prima di effettuare l'acquisto automatico il sistema deposita, sul portafoglio dell'utente, un ammontare di valuta fiat pari al budget da lui scelto | Funzionale |
| R1NF | Velocità di memorizzazione e recupero dati | Non Funzionale |
| R2NF | Il sistema deve garantire la velocità di recupero dei dati anche in caso di grandi quantità di dati | Non Funzionale |
| R3NF | Semplicità di utilizzo delle diverse maschere del sistema | Non Funzionale |
| R4NF | Il sistema deve garantire la disponibilità anche in caso di grosse moli di dati in trasferimento | Non Funzionale |
| R5NF | Il sistema deve garantire una latenza minima nell'aggiornamento dei valori delle criptovalute | Non Funzionale |
| R6NF | Va garantita la protezione dei dati inseriti dagli utenti | Non Funzionale |
| R7NF | Non può succedere che un utente acquisti criptovalute non disponibili per la propria valuta fiat di riferimento | Non Funzionale |

Analisi del Dominio

Vocabolario

| Voce | Definizione | Sinonimi |
|-----------------------------|--|-------------------------------|
| Dollar Cost Averaging (DCA) | Strategia che consiste nell'Investimento di una somma di denaro prestabilita in acquisti periodici diversificati per ridurre l'impatto della volatilità dei Beni | Strategia DCA |
| Piattaforma di Exchange | Strumento tecnologico che permette di acquistare e vendere Criptovalute | |
| Criptovaluta | Moneta elettronica e decentralizzata basata su crittografia asimmetrica | Valuta digitale, Bene, Moneta |
| Portafoglio | Servizio per conservare, su cui depositare e da cui ritirare Valute Digitali e/o Valuta Fiat | |
| Utente | Utilizzatore delle funzionalità offerte dal sistema | |
| Andamento | L'evoluzione nel tempo del valore del Portafoglio dell'Utente | |
| Interfaccia grafica | Finestre mediante la quale l'Utente sfrutta le funzionalità del sistema | |
| Investimento | Impiego di una somma di denaro per l'acquisto di Beni finalizzato al guadagno, effettuato in maniera automatica dal sistema | Spesa, Transazione, Ordine |
| Distribuzione Percentuale | Insieme di percentuali di Budget assegnate a ciascuna Criptovaluta | Distribuzione |
| Registrazione | Azione attraverso la quale un Utente ottiene l'abilitazione all'utilizzo del sistema | Iscrizione |
| Username | Sequenza di caratteri univoca che identifica un Utente | |
| Password | Codice segreto scelto da un Utente | |
| Accesso | Recupero dei dati dell'Utente a seguito dell'immissione delle sue Credenziali | Login, Autenticazione |

| | | |
|----------------------------|--|------------------------------------|
| Posta Elettronica | Stringa alfanumerica specificata dall'Utente in fase di Registrazione per ricevere comunicazioni da parte del sistema | Indirizzo Email |
| Credenziali | Username e Password usate per l'autenticazione nell'applicazione | |
| Valuta Fiat | Denaro emesso da stati e banche centrali | Denaro |
| Valuta Fiat di Riferimento | Valuta Fiat rispetto alla quale vengono visualizzati i dati relativi al Portafoglio dell'Utente e il valore delle Criptovalute | Valuta di Riferimento |
| Cronologia degli acquisti | Insieme di Riepiloghi dell'Ordine | Storico delle Transazioni, Storico |
| Amministratore | Utente con privilegi speciali | |
| Tetto di Spesa | Soglia massima che viene investita, nell'attuare la strategia DCA, per l'acquisto delle criptovalute ad ogni Intervallo di Investimento | Budget, Disponibilità |
| Deposito | Azione attraverso la quale viene aumentata la Disponibilità di Valuta Fiat sul Portafoglio dell'Utente | |
| Resoconto | Documento che riporta: <ul style="list-style-type: none"> • La variazione del valore del Portafoglio rispetto al primo giorno dello specifico mese • La Spesa totale complessiva effettuata nello specifico mese • La Spesa per ogni Moneta effettuata nello specifico mese | |
| Terminazione | Annullamento della Registrazione, dopo il quale i servizi del sistema non sono più fruibili dall'Utente. Comporta l'eliminazione dei dati dell'Utente | |
| Intervallo di Investimento | Lasso di tempo tra due Investimenti automatici, scelto dall'Utente | Frequenza temporale di acquisto |
| Intervallo Aggiornamento | Intervallo di 30 secondi per l'aggiornamento dei dati delle | |

| | | |
|---|---|-----------------------|
| | criptovalute | |
| Codice di Verifica | Sequenza di caratteri casuali | |
| Riepilogo dell'Ordine | <p>Descrizione dell'acquisto automatico effettuato dal sistema, rappresentato da:</p> <ul style="list-style-type: none"> • la data in cui è stato effettuato • il quantitativo di Valuta Fiat utilizzato • l'ammontare di Criptovaluta/e acquistata/e • il valore della/e Criptovaluta/e al momento dell'Investimento | Riepilogo Ordine |
| Parametri di Investimento | Insieme di Intervallo di Investimento e Budget | |
| Metodo di Pagamento | Informazioni utilizzate per effettuare i depositi in Valuta Fiat e gli Investimenti sul Portafoglio dell'Utente | |
| Percentuale di Budget assegnata alla Criptovaluta | Percentuale del Budget che l'Utente assegna ad ogni Criptovaluta da lui scelta; utilizzata per determinare quanto Budget è impiegato per comprare la Criptovaluta ad ogni attuazione della strategia di DCA | Percentuale Assegnata |
| Previsione della Spesa | Spesa in Valuta Fiat per un dato periodo di tempo, calcolata in base a Budget e Intervallo di Investimento | |

Sistemi Esterni

Il software dovrà interfacciarsi con un servizio online che offre la gestione di un portafoglio di criptovalute e dal quale inoltre verranno effettuati gli investimenti e i depositi.

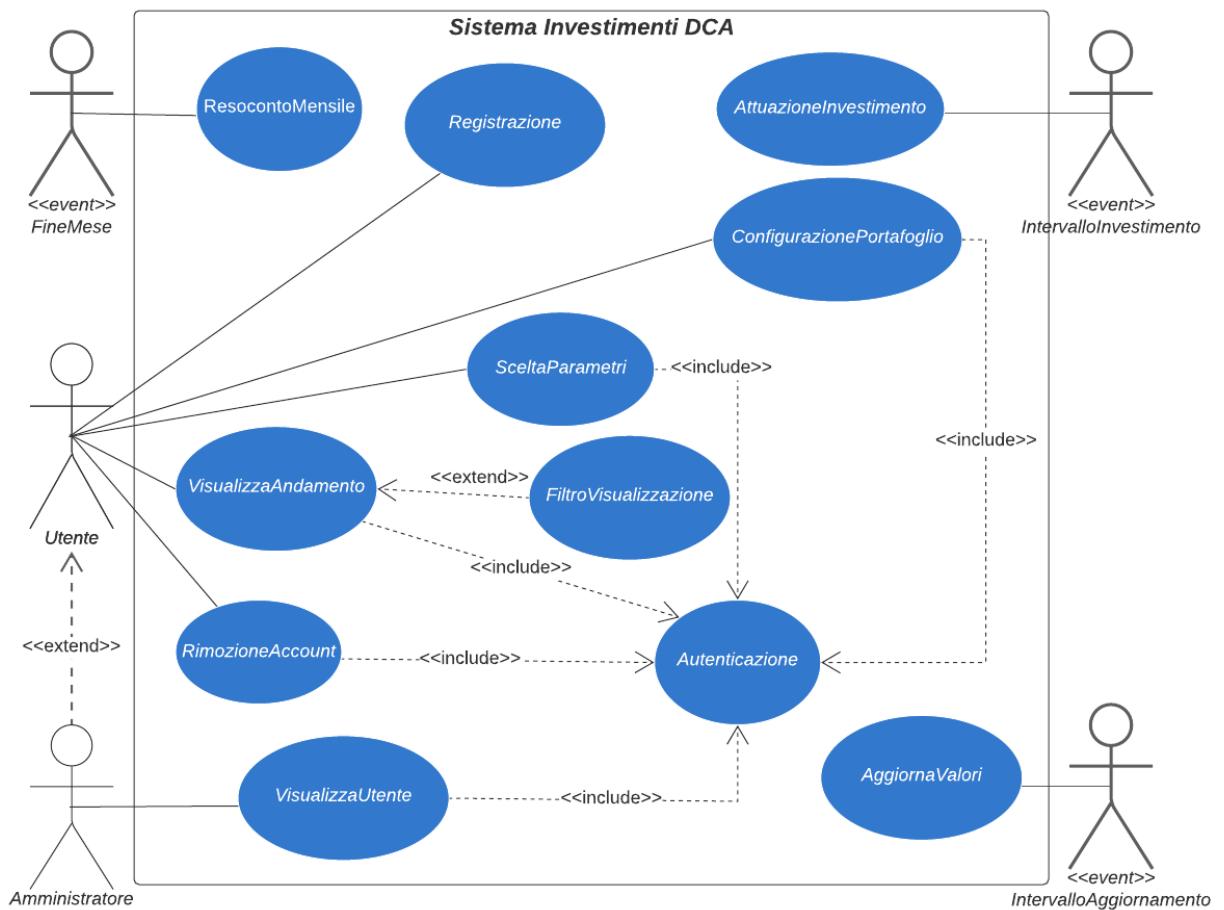
Sarà inoltre anche necessario un servizio per gestire l'invio di email.

Analisi dominio applicativo

Il sistema, per funzionare, dovrà fare affidamento su di una piattaforma online che dia la possibilità di gestire completamente e autonomamente un portafoglio di criptovalute con la possibilità di effettuare nuovi investimenti e depositi di valuta fiat. Inoltre ci aspettiamo che questa piattaforma dia la possibilità di accedere anche ai dati e ai valori in tempo reale delle criptovalute, i quali dovranno essere sincronizzati e salvati nel sistema.

Analisi Requisiti

Modello dei Casi d'Uso



Scenari

| | |
|---------------------------------|---|
| Titolo | Registrazione |
| Descrizione | L'Utente si registra per poter usufruire dei servizi del sistema |
| Attori | Utente |
| Relazioni | |
| Precondizioni | |
| Postcondizioni | L'Utente può effettuare l'Autenticazione con le sue Credenziali |
| Scenario principale | <ol style="list-style-type: none"> 1. All'Utente viene mostrata la schermata di registrazione 2. L'Utente inserisce uno Username, una Password, un Indirizzo Email, una Valuta di Riferimento e un Metodo di Pagamento nei campi appositi 3. Il sistema verifica che i dati inseriti siano validi 4. Il sistema invia un messaggio di posta elettronica, all'Indirizzo Email indicata dall'Utente, con un Codice di Verifica 5. L'Utente inserisce il Codice di Verifica 6. I dati dell'Utente vengono memorizzati nel sistema 7. Viene visualizzato un messaggio di benvenuto |
| Scenari alternativi | <p>Scenario a: L'Utente inserisce uno Username o un Indirizzo Email già memorizzati nel sistema</p> <ol style="list-style-type: none"> 1. Viene mostrato un messaggio di errore 2. L'Utente deve inserire nuovamente i dati per la registrazione, rimanendo così nel passo 2 dello scenario principale <p>Scenario b: Codice di Verifica errato</p> <ol style="list-style-type: none"> 1. Viene mostrato un messaggio di errore 2. L'Utente può modificare l'Indirizzo Email o richiedere un nuovo Codice di Verifica 3. Viene eseguito nuovamente il punto 4 |
| Requisiti non funzionali | Protezione dei dati inseriti |
| Punti Aperti | |

| | |
|---------------------------------|--|
| Titolo | AggiornaValori |
| Descrizione | Il sistema cerca di aggiornare i valori delle Criptovalute |
| Attori | IntervalloAggiornamento |
| Relazioni | |
| Precondizioni | |
| Postcondizioni | I valori delle Criptovalute memorizzati nel sistema sono aggiornati |
| Scenario principale | <ol style="list-style-type: none"> 1. Si verifica l'evento IntervalloAggiornamento 2. Il sistema recupera i valori attuali delle Criptovalute dalla Piattaforma di Exchange 3. Il sistema memorizza i valori aggiornati delle Criptovalute appena scaricati |
| Scenari alternativi | <p>Scenario a: Il recupero dei nuovi valori delle Criptovalute fallisce</p> <ol style="list-style-type: none"> 1. Il sistema non memorizza nessun nuovo dato |
| Requisiti non funzionali | Il recupero e la modifica dei valori devono richiedere un tempo molto minore rispetto all'Intervallo di Aggiornamento |
| Punti Aperti | |

| | |
|----------------------------|--|
| Titolo | ResocontoMensile |
| Descrizione | Il sistema cerca di produrre un Resoconto che descrive le variazioni del Portafoglio dell'Utente nell'ultimo mese |
| Attori | FineMese |
| Relazioni | |
| Precondizioni | L'Utente deve essere registrato nel sistema Deve essere stato effettuato almeno un acquisto automatico da parte del sistema |
| Postcondizioni | All'Utente arriva nella casella di posta elettronica il documento prodotto |
| Scenario principale | <ol style="list-style-type: none"> 1. Si verifica l'evento FineMese 2. Il sistema recupera i Riepiloghi degli Ordini dal primo all'ultimo giorno del mese per ogni Utente 3. Per ogni Utente il sistema calcola: <ul style="list-style-type: none"> • La variazione del valore del Portafoglio rispetto |

| | |
|---------------------------------|--|
| | <p>al primo giorno dello specifico mese</p> <ul style="list-style-type: none"> ● La Spesa totale complessiva effettuata nello specifico mese ● La Spesa per ogni Moneta effettuata nello specifico mese <ol style="list-style-type: none"> 4. I dati calcolati vengono utilizzati per produrre un Resoconto per ogni Utente 5. Il sistema invia un messaggio di Posta Elettronica all'Indirizzo Email specificato da ogni Utente con il Resoconto prodotto per l'Utente in questione |
| Scenari alternativi | |
| Requisiti non funzionali | |
| Punti Aperti | |

| | |
|---------------------------------|---|
| Titolo | Autenticazione |
| Descrizione | Offre la possibilità all'Utente e all'Amministratore di autenticarsi e farsi identificare dal sistema in modo tale da poter accedere alle sue funzionalità |
| Attori | Utente, Amministratore |
| Relazioni | VisualizzaAndamento, RimozioneAccount, VisualizzaUtente, SceltaParametri, ConfigurazionePortafoglio |
| Precondizioni | |
| Postcondizioni | |
| Scenario principale | <ol style="list-style-type: none"> 1. Viene presentata una maschera per l'inserimento delle Credenziali 2. L'Utente o l'Amministratore inseriscono le Credenziali 3. Il sistema verifica che le Credenziali inserite siano associate ad un Utente registrato 4. Viene presentata la maschera principale del sistema |
| Scenari alternativi | Scenario a: Credenziali non riconosciute <ol style="list-style-type: none"> 1. Viene mostrato un messaggio di errore 2. L'Utente o l'Amministratore devono reinserire le Credenziali |
| Requisiti non funzionali | Bisogna garantire la riservatezza dei dati inseriti |
| Punti Aperti | In fase di progettazione gestiremo il fatto che non debba essere richiesta l'autenticazione per tutte le interazioni per una stessa sessione dell'Utente |

| | |
|---------------------------------|---|
| Titolo | VisualizzaAndamento |
| Descrizione | L'Utente può interfacciarsi con i dati che rappresentano l'evoluzione del valore del Portafoglio e lo Storico |
| Attori | Utente |
| Relazioni | FiltroVisualizzazione, Autenticazione |
| Precondizioni | |
| Postcondizioni | Vengono mostrati all'Utente tutti i dati da lui richiesti |
| Scenario principale | <ol style="list-style-type: none"> 1. Autenticazione 2. Il sistema recupera la Cronologia degli Acquisti relativa all'Utente 3. Il sistema calcola l'evoluzione del valore del Portafoglio in base alla Valuta Fiat di Riferimento dell'Utente 4. Il sistema calcola il valore attuale del Portafoglio in Valuta Fiat di Riferimento 5. Il sistema mostra a video l'evoluzione del valore del Portafoglio su di un grafico 6. Il sistema mostra a video la Cronologia degli Acquisti e il valore attuale in Valuta Fiat di Riferimento del Portafoglio 7. L'Utente può scegliere di applicare filtri ai dati tramite FiltroVisualizzazione |
| Scenari alternativi | |
| Requisiti non funzionali | Velocità di recupero dati |
| Punti Aperti | |

| | |
|---------------------------------|---|
| Titolo | FiltroVisualizzazione |
| Descrizione | L'Utente ha la possibilità di restringere il campo di ricerca dei dati e grafici visualizzati |
| Attori | Utente |
| Relazioni | VisualizzaAndamento |
| Precondizioni | |
| Postcondizioni | Il filtro viene applicato |
| Scenario principale | <ol style="list-style-type: none"> 1. L'Utente può decidere di applicare filtri per: <ul style="list-style-type: none"> • Moneta • Intervallo di date • Spesa in Valuta Fiat di Riferimento 2. Lo Storico e il grafico dell'Andamento mostrati vengono aggiornati con i filtri inseriti |
| Scenari alternativi | |
| Requisiti non funzionali | Velocità di recupero dati |
| Punti Aperti | |

| | |
|---------------------------------|---|
| Titolo | SceltaParametri |
| Descrizione | Configurazione dei Parametri di Investimento utilizzati per attuare la strategia DCA |
| Attori | Utente |
| Relazioni | Autenticazione |
| Precondizioni | |
| Postcondizioni | I Parametri di Investimento vengono aggiornati |
| Scenario principale | <ol style="list-style-type: none"> 1. Autenticazione 2. Il sistema scarica e mostra, se già configurati un'altra volta, all'Utente il valore attuale dell'Intervallo di Investimento e il Budget 3. Viene mostrata una maschera per l'inserimento o la modifica dell'Intervallo di Investimento (in giorni) e del Budget 4. Il sistema memorizza i Parametri di Investimento se inseriti 5. Il sistema mostra una Previsione della Spesa futura dell'Utente nei prossimi 12 mesi rispetto al Budget e all'Intervallo di Investimento |
| Scenari alternativi | |
| Requisiti non funzionali | |
| Punti Aperti | |

| | |
|---------------------------------|---|
| Titolo | ConfigurazionePortafoglio |
| Descrizione | L'Utente sceglie la propria Distribuzione Percentuale |
| Attori | Utente |
| Relazioni | Autenticazione |
| Precondizioni | |
| Postcondizioni | Viene aggiornata la Distribuzione Percentuale scelta dall'Utente |
| Scenario principale | <ol style="list-style-type: none"> 1. Autenticazione 2. Il sistema recupera e mostra una lista delle Criptovalute acquistabili dall'Utente con la sua Valuta Fiat di Riferimento e la Distribuzione Percentuale attuale, se già impostata 3. L'Utente sceglie una o più Criptovalute tra quelle disponibili nella lista 4. L'Utente assegna a ciascuna Criptovaluta scelta la percentuale che occuperà nel Budget 5. Il sistema aggiorna la Distribuzione Percentuale scelta dall'Utente |
| Scenari alternativi | |
| Requisiti non funzionali | Non può succedere che un Utente scelga Criptovalute non disponibili per la propria Valuta Fiat di Riferimento |
| Punti Aperti | |

| | |
|----------------------------|--|
| Titolo | RimozioneAccount |
| Descrizione | L'Utente chiede la Terminazione |
| Attori | Utente |
| Relazioni | Autenticazione |
| Precondizioni | |
| Postcondizioni | La Terminazione viene eseguita |
| Scenario principale | <ol style="list-style-type: none"> 1. Autenticazione 2. All'Utente viene mostrata una maschera dalla quale confermare la volontà di Terminazione 3. L'Utente viene de-autenticato 4. Il sistema elimina tutti i dati relativi all'Utente 5. L'Utente viene riportato alla Registrazione |

| | |
|---------------------------------|--|
| Scenari alternativi | Scenario a: L'Utente non conferma la volontà di Terminazione 1. L'Utente viene de-autenticato e i suoi dati rimangono salvati |
| Requisiti non funzionali | |
| Punti Aperti | |

| | |
|---------------------------------|---|
| Titolo | AttuazioneInvestimento |
| Descrizione | La strategia DCA viene applicata sul Portafoglio dell'Utente effettuando gli Acquisti delle Criptovalute sulla Piattaforma di Exchange |
| Attori | IntervalloInvestimento |
| Relazioni | |
| Precondizioni | L'Utente deve aver definito un Budget, un Intervallo di Investimento e una Distribuzione Percentuale per il suo Portafoglio |
| Postcondizioni | Le Criptovalute sono aggiunte al Portafoglio dell'Utente |
| Scenario principale | <ol style="list-style-type: none"> 1. Si verifica l'evento IntervalloInvestimento 2. Il sistema si collega remotamente al Portafoglio dell'Utente sulla Piattaforma di Exchange 3. Il sistema calcola, rispetto alla Distribuzione Percentuale, quanta Valuta Fiat di Riferimento va investita per ogni Criptovaluta scelta dall'Utente 4. Il sistema deposita, tramite il Metodo di Pagamento scelto, un quantitativo di Valuta Fiat pari al Budget sul Portafoglio dell'Utente 5. Il sistema acquista ciascuna Criptovaluta in base al calcolo appena effettuato 6. Il sistema memorizza il Riepilogo dell'Ordine |
| Scenari alternativi | <p>Scenario a: fondi insufficienti per effettuare il Deposito</p> <ol style="list-style-type: none"> 1. L'investimento non viene effettuato 2. Viene inviato un messaggio di Posta Elettronica all'Indirizzo Email dell'Utente che segnala il fallimento dell'acquisto |
| Requisiti non funzionali | Protezione dei dati |
| Punti Aperti | |

| | |
|---------------------------------|--|
| Titolo | VisualizzaUtente |
| Descrizione | L'Amministratore visualizza i Riepiloghi degli Ordini degli Utenti |
| Attori | Amministratore |
| Relazioni | Autenticazione |
| Precondizioni | |
| Postcondizioni | |
| Scenario principale | <ol style="list-style-type: none"> 1. Autenticazione 2. Il sistema recupera l'elenco degli Utenti registrati 3. Viene mostrato l'elenco recuperato 4. L'Amministratore sceglie un Utente tra quelli presenti nell'elenco 5. Il sistema mostra i Riepiloghi degli Ordini dell'Utente selezionato |
| Scenari alternativi | <p>Scenario a: L'Utente non ha effettuato alcun Ordine</p> <ol style="list-style-type: none"> 1. Viene mostrato un messaggio di errore 2. L'Amministratore può selezionare un altro Utente |
| Requisiti non funzionali | Velocità di recupero dei dati |
| Punti Aperti | |

Analisi del rischio

Valutazione dei beni

| Bene | Valore | Esposizione |
|--|---|---|
| Sistema Informativo | Alto. Supporto alla gestione dei dati utilizzati in molte delle funzionalità offerte dal sistema. Supporto per l'attuazione automatica degli investimenti. | Alta. Perdita economica e costi di ripristino. Perdita d'immagine se la notizia diventa di pubblico dominio. |
| Informazioni relative agli utenti | Alto. Informazioni di carattere economico legate all'utente: metodo di pagamento contenente i dati per la connessione al portafoglio | Molto Alta. Rischio di grave perdita d'immagine e finanziaria se i dati vengono divulgati. Grave rischio economico e finanziario anche per gli utenti coinvolti. Rischio di utilizzo non autorizzato del sistema con i dati divulgati |
| Informazioni relative agli ordini | Basso. Non contiene informazioni sensibili o economiche, ma solo riepiloghi di acquisti. | Media. Perdita d'immagine. Dubbio sulla veridicità dei riepiloghi dei dati mostrati se attacco all'integrità dei dati. |
| Informazioni relative alle criptovalute | Molto Basso. Informazioni facilmente reperibili online. | Bassa. Non influisce con gli acquisti e gli investimenti. Se i dati perdono integrità: riepiloghi degli ordini non corretti e di conseguenza resoconti e andamenti mostrati potrebbero non essere veritieri |
| Informazioni relative all'amministratore | Medio. Essendo un utente potrebbe avere informazioni economiche. Dal punto di vista dei privilegi basso perché non ha permessi particolari di modifica dei dati. | Medio. Non vengono causati danni al sistema. Media, dal punto di vista dei dati privati come utente. Perdita d'immagine. |
| Informazioni sui parametri di investimento e distribuzione percentuale | Medio. Dati che rappresentano come gli utenti desiderano effettuare gli investimenti. | Alto. Rischio di effettuare acquisti e depositi secondo parametri non impostati dall'utente. Perdita d'immagine |

Tabella minacce/controlli

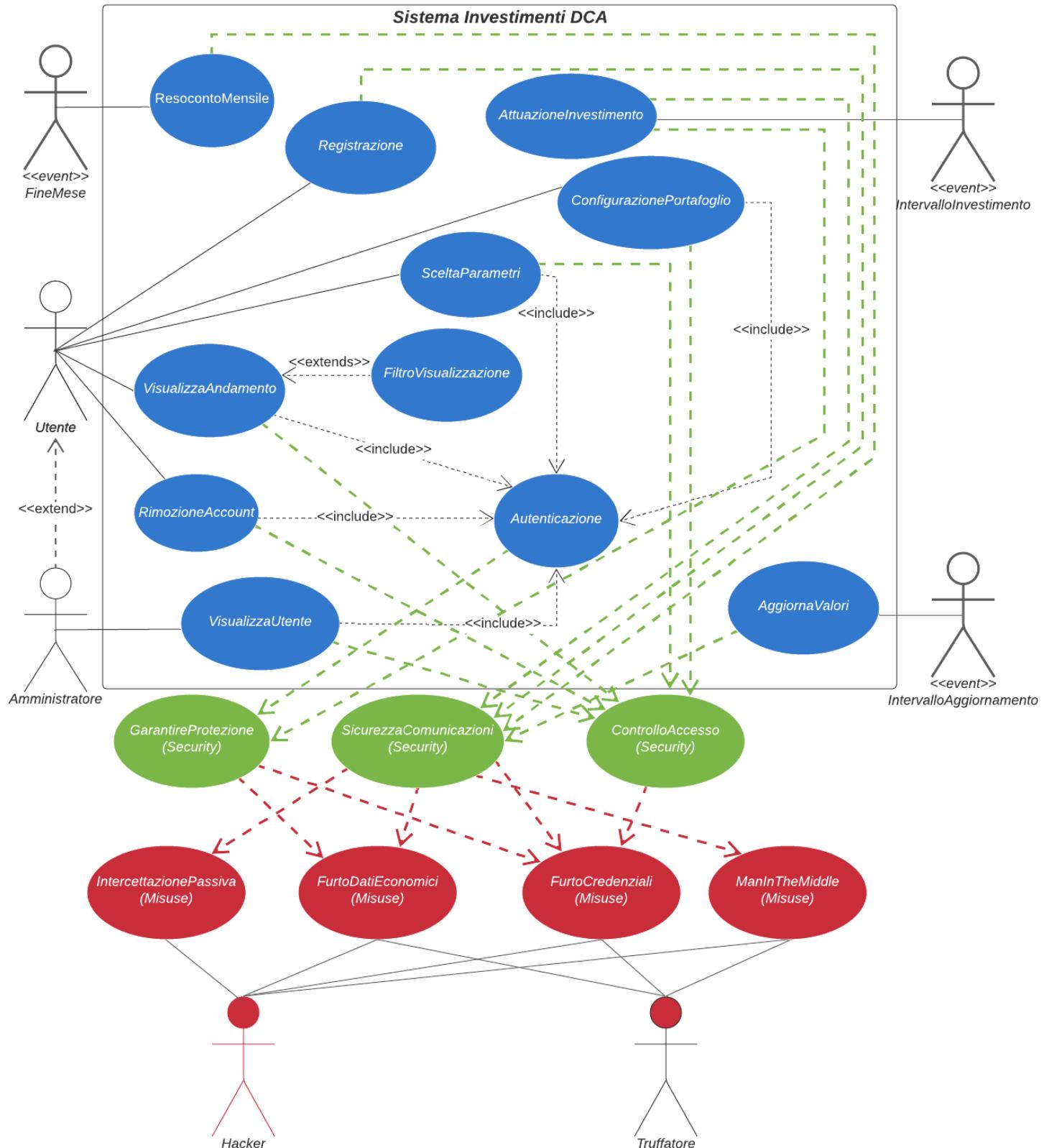
| Minaccia | Probabilità | Controllo | Fattibilità |
|--|--|---|---|
| Intercettazione passiva del traffico e alterazione comunicazioni | Alta. Le interazioni degli utenti con il sistema saranno di tipo client/server remoto | Utilizzo di canali sicuri e certificati per la comunicazione | Basso costo implementativo ed economico |
| | | Log delle operazioni | Basso costo di implementazione |
| Furto credenziali utente | Alta. L'utente deve inviare le proprie credenziali ad ogni nuovo utilizzo del sistema. Rischio che l'utente usi le stesse credenziali per altri servizi vulnerabili | Dopo alcuni tentativi errati viene bloccato l'accesso | Basso costo di implementazione |
| | | Log di ogni operazione e degli indirizzi IP | Basso costo di implementazione |
| Furto credenziali amministratore | Media. Numero di amministratori molto minore di quello degli utenti | Utilizzo stesse logiche di controllo per il furto delle credenziali dell'utente | Basso costo di implementazione |
| Modifica e furto dei dati economici degli utenti | Media. Dati scambiati in fase di registrazione e poi memorizzati dal sistema. Dati usati dal sistema per attuare investimenti e/o depositi | Cifratura dei dati salvati nel sistema | Potenza di calcolo richiesta dipendente dall'algoritmo e dalla lunghezza della chiave |
| DoS | Media. Possibilità di traffico elevato in fase di impostazione parametri e visualizzazione andamento | Adeguata progettazione del sistema e limitazione delle operazioni effettuabili | Costo medio. Vari scenari di attacco possibili, difficile proteggersi da tutti |

Analisi delle tecnologie della sicurezza

| Tecnologia | Vulnerabilità |
|--|---|
| Architettura Client/Server | <ul style="list-style-type: none"> • Attacco Man in the Middle • Attacchi alla disponibilità del server • Intercettazione delle comunicazioni • Accesso a funzionalità del sistema senza autorizzazioni |
| Cifratura | dei dati |
| | delle comunicazioni |
| Autenticazione con credenziali | <p>In caso di cifratura simmetrica:</p> <ul style="list-style-type: none"> • Memorizzazione della chiave, da mantenere su supporti fisici sicuri • Tempo di vita della chiave, sarebbe consigliato cambiarla periodicamente per evitare analisi dei dati cifrati • Lunghezza della chiave, consigliato l'utilizzo di chiave robusta a 256/512 bit per evitare attacchi di forza bruta <p>In caso di cifratura asimmetrica:</p> <ul style="list-style-type: none"> • Memorizzazione chiave privata, va mantenuta al sicuro. Può essere usata per impersonare il sistema • Autenticità del certificato |
| Elementi di input per l'inserimento dei dati | <ul style="list-style-type: none"> • Attacchi di Buffer Overflow • Iniezione di codice malevolo |

Security Use Case e Misuse Case

Modello



Scenari

| | | |
|--|---|--|
| Titolo | SicurezzaComunicazioni | |
| Descrizione | Tutti i dati trasmessi tra il sistema e gli utenti dovrebbero rimanere integri e riservati | |
| Misuse | IntercettazionePassiva, ManInTheMiddle, FurtoCredenziali, FurtoDatiEconomici | |
| Precondizioni | <ol style="list-style-type: none"> 1. L'Attaccante ha la capacità di intercettare le comunicazioni 2. L'Attaccante ha la capacità di modificare i dati intercettati 3. L'Attaccante ha la possibilità di inviare il messaggio modificato | |
| Postcondizioni | Il sistema segnala il tentativo di attacco | |
| Scenario principale | <i>Sistema</i> | <i>Attaccante</i> |
| | Cerca di garantire che i dati inviati all'Utente siano protetti e non possano essere modificati | |
| | | Intercetta un messaggio, ma non può decifrarlo |
| | | Cerca di inviare un messaggio fraudolento all'Utente o al Sistema |
| Scenario di attacco avvenuto con successo | Il Sistema si accorge della discrepanza e segnala un tentativo di frode | |
| | <i>Sistema</i> | <i>Attaccante</i> |
| | Cerca di garantire che i dati inviati all'Utente siano protetti e non possano essere modificati | |
| | | Intercetta un messaggio e riesce a decifrarlo ed analizzarlo |
| | | L'attaccante invia un messaggio al sistema, per eseguire operazioni malevoli |
| | Tutte le operazioni e le relative informazioni che avvengono nel sistema sono salvate nei log. Periodicamente vengono | |

| | | |
|--|---|--|
| | <p>cercate, dal sistema, discrepanze e frodi nelle operazioni salvate nei log.</p> <p>In caso di potenziale frode il sistema produce una segnalazione visionabile da un amministratore addetto alla sicurezza</p> | |
|--|---|--|

| | | |
|--|---|---|
| Titolo | GarantireProtezione | |
| Descrizione | Bisogna garantire che utenti malintenzionati non possano accedere, analizzare e/o modificare i dati salvati nel sistema | |
| Misuse | FurtoDatiEconomici, FurtoCredenziali | |
| Precondizioni | 1. L'Attaccante ha i mezzi e le possibilità di cercare e sfruttare eventuali vulnerabilità presenti nel sistema | |
| Postcondizioni | Il Sistema blocca ogni tentativo di attacco ai dati da parte dell'Attaccante | |
| Scenario principale | <i>Sistema</i> | <i>Attaccante</i> |
| | Cerca di garantire che i dati sensibili ed economici salvati siano al sicuro | |
| | Garantisce la cifratura dei dati | |
| | | Cerca delle vulnerabilità per superare le difese del sistema, ma non ne trova |
| Scenario di attacco avvenuto con successo | <i>Sistema</i> | <i>Attaccante</i> |
| | Garantisce che i dati sensibili ed economici salvati siano cifrati in maniera robusta | |
| | Cerca di garantire la sicurezza da vulnerabilità | |
| | | Cerca e trova delle vulnerabilità per superare le difese del sistema |

| | | |
|--|---|--|
| | | L'attaccante accede ai dati sensibili ed economici, che sono però cifrati in maniera robusta |
| | Il sistema salva nel log gli accessi effettuati ai dati. L'Amministratore analizza i log alla ricerca di accessi non autorizzati | |

| | | |
|--|---|---|
| Titolo | ControlloAccesso | |
| Descrizione | Ogni accesso al sistema deve essere controllato | |
| Misuse | FurtoCredenziali | |
| Precondizioni | 1. L'Attaccante ha gli strumenti per tentare di autenticarsi con le Credenziali di altri Utenti | |
| Postcondizioni | Il Sistema blocca il tentativo di accesso all'Attaccante non autorizzato | |
| Scenario principale | <i>Sistema</i> | <i>Attaccante</i> |
| | | Cerca di individuare ed inserire più volte le Credenziali di un altro Utente, ma le Credenziali sono errate |
| | Viene bloccato l'accesso e la possibilità di effettuare ulteriori tentativi. Viene prodotta una segnalazione | |
| Scenario di attacco avvenuto con successo | <i>Sistema</i> | <i>Attaccante</i> |
| | | Individua ed inserisce delle Credenziali corrette |
| | Il sistema permette l'accesso | |
| | | Può effettuare tutte le operazioni che vuole all'interno dell'account dell'Utente |
| | Tutte le operazioni e le relative informazioni che avvengono nel sistema sono salvate nei log. Periodicamente vengono cercate, | |

| | | |
|--|---|--|
| | dal sistema, discrepanze e pattern inconsueti nelle operazioni salvate nei log. | |
|--|---|--|

Requisiti di sicurezza

Dall'analisi del rischio è emersa la necessità di implementare ulteriori requisiti per migliorare la protezione del sistema:

| ID | Requisito | Tipo |
|-------|---|----------------|
| RS1F | Creazione di log, che non devono contenere dati economici e sensibili, il cui obiettivo è quello di tenere traccia di: <ul style="list-style-type: none"> • Operazioni svolte nel sistema • Accessi effettuati ai dati sensibili ed economici | Funzionale |
| RS2F | Implementazione di meccanismi per l'analisi dei log che cerchino di individuare eventuali discrepanze e pattern insoliti negli accessi e nelle operazioni | Funzionale |
| RS3F | L'Amministratore avrà accesso ai log per effettuare le analisi e gestirà eventuali segnalazioni di eventi sospetti da parte del sistema | Funzionale |
| RS1NF | I dati memorizzati nel sistema e quelli scambiati vanno protetti | Non Funzionale |

Analisi del problema

Analisi delle Funzionalità

Tabella delle Funzionalità

| Funzionalità | Tipo | Grado Complessità | Requisiti Collegati |
|---------------------------|---|-------------------|---------------------|
| VisualizzaAndamento | Gestione dati | Semplice | R3F, R14F, R9F |
| SceltaParametri | Gestione dati, Memorizzazione dati | Semplice | R4F, R7F |
| ConfigurazionePortafoglio | Gestione dati, Memorizzazione dati | Semplice | R15F, R5F |
| Registrazione | Gestione dati, Memorizzazione dati, Interazione con l'esterno | Complessa | R6F |
| Autenticazione | Gestione dati | Semplice | R16F |
| RimozioneAccount | Cancellazione dati | Semplice | R13F |
| ResocontoMensile | Gestione dati, Interazione con l'esterno | Semplice | R11F, R12F |
| AttuazioneInvestimento | Gestione dati, Memorizzazione dati, Interazione con l'esterno | Complessa | R1F, R8F, R17F |
| AggiornaValori | Memorizzazione dati, Interazione con l'esterno | Semplice | R2F |
| VisualizzaUtente | Gestione dati | Semplice | R10F |
| CreazioneLog | Memorizzazione dati | Semplice | RS1F |
| AnalisiLog | Gestione dati | Semplice | RS2F |
| VisualizzaLog | Gestione dati | Semplice | RS3F |

VisualizzaAndamento: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|---------------------|----------|----------------------------|--------------|---------|
| Riepilogo Ordine | Composto | Alta | Input | |
| Valore Portafoglio | Semplice | Alta | Output | |
| Nome Criptovaluta | Semplice | Bassa | Input | |
| Valore Criptovaluta | Semplice | Bassa | Input | |
| Intervallo di date | Semplice | Bassa | Input | |
| Importo della Spesa | Semplice | Bassa | Input | |

SceltaParametri: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|----------------------------|----------|----------------------------|--------------|---------|
| Intervallo di Investimento | Semplice | Media | Input | |
| Budget | Semplice | Media | Input | |
| Previsione Spesa | Semplice | Alta | Output | |

ConfigurazionePortafoglio: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|---|----------|----------------------------|--------------|---------|
| Nome Criptovaluta | Semplice | Media | Input | |
| Percentuale di Budget assegnata alla Criptovaluta | Semplice | Media | Input | |

Note: La lista delle Criptovalute supportate per la Valuta Fiat di Riferimento dell'Utente viene utilizzata per controllare che il Nome della Criptovaluta che sceglie sia tra quelle

Registrazione: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|-----------------------|-------------|-----------------------------------|---------------------|--|
| Username | Semplice | Alta | Input | Non più di 32 caratteri |
| Password | Semplice | Molto Alta | Input | Non più di 64 caratteri e più di uno maiuscolo |
| Indirizzo Email | Semplice | Alta | Input | |
| Valuta di Riferimento | Semplice | Bassa | Input | |
| Metodo di Pagamento | Composto | Molto Alta | Input | |
| Codice di Verifica | Semplice | Media | Input | 6 caratteri |

Autenticazione: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|---------------------|-------------|-----------------------------------|---------------------|--|
| Username | Semplice | Alta | Input | Non più di 32 caratteri |
| Password | Semplice | Molto Alta | Input | Non più di 64 caratteri, almeno un carattere maiuscolo |

RimozioneAccount: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|---------------------|-------------|-----------------------------------|---------------------|-------------------------|
| Username | Semplice | Alta | Input | Non più di 32 caratteri |

ResocontoMensile: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|------------------|----------|----------------------------|--------------|---------|
| Data inizio mese | Semplice | Bassa | Input | |
| Data fine mese | Semplice | Bassa | Input | |
| Riepilogo Ordine | Composto | Alta | Input | |
| Indirizzo Email | Semplice | Alta | Input | |
| Resoconto | Composto | Alta | Output | |

AttuazioneInvestimento: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|-----------------------|----------|----------------------------|--------------|---------|
| Metodo di Pagamento | Composto | Molto Alta | Input | |
| Budget | Semplice | Media | Input | |
| Nome Criptovaluta | Semplice | Media | Input | |
| Percentuale Assegnata | Semplice | Media | Input | |
| Riepilogo Ordine | Composto | Alta | Output | |
| Indirizzo Email | Semplice | Alta | Input | |

Note:

L'Indirizzo Email sarà necessario solo per lo scenario alternativo, nel caso in cui i fondi per effettuare il Deposito siano insufficienti

AggiornaValori: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|-------------------------------------|----------|----------------------------|--------------|---------|
| Data | Semplice | Bassa | Input | |
| Ora | Semplice | Bassa | Input | |
| Criptovaluta Composta da: | Compusto | Bassa | Input | |
| Nome | Semplice | Bassa | Input | |
| Sigla | Semplice | Bassa | Input | |
| Valore | Semplice | Bassa | Input | |

VisualizzaUtente: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|------------------|----------|----------------------------|--------------|-------------------------|
| Username | Semplice | Alta | Input | Non più di 32 caratteri |
| Riepilogo Ordine | Compusto | Alta | Output | |

CreazioneLog: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|-----------------|----------|----------------------------|--------------|---------|
| Data | Semplice | Media | Input | |
| Ora | Semplice | Media | Input | |
| Tipo Operazione | Compusto | Alta | Input | |
| Messaggio | Semplice | Alta | Input | |

AnalisiLog: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|---------------------|-------------|-----------------------------------|---------------------|----------------|
| Log | Composto | Alta | Input | |
| Segnalazione | Composto | Alta | Output | |

VisualizzaLog: Tabella Informazioni/Flusso

| Informazione | Tipo | Livello protezione/privacy | Input/Output | Vincoli |
|---------------------|-------------|-----------------------------------|---------------------|----------------|
| Data | Semplice | Media | Output | |
| Ora | Semplice | Media | Output | |
| Tipo Operazione | Composto | Alta | Output | |
| Messaggio | Semplice | Alta | Output | |

Analisi dei vincoli

Tabella vincoli

| Requisito | Categorie | Impatto | Funzionalità |
|---------------------------------|-------------------|--|---|
| Velocità memorizzazione dati | Tempo di risposta | Cercare di migliorare | SceltaParametri, ConfigurazionePortafoglio, Registrazione, AggiornaValori, CreazioneLog |
| Velocità ricerca dati | Tempo di risposta | Cercare di migliorare | VisualizzaAndamento, SceltaParametri, ConfigurazionePortafoglio, Autenticazione, VisualizzaUtente, AnalisiLog, VisualizzaLog |
| Semplicità di utilizzo maschere | Usabilità | Miglioramento dell'esperienza utente | VisualizzaAndamento, SceltaParametri, ConfigurazionePortafoglio, Registrazione, Autenticazione |
| Garantire disponibilità | Disponibilità | Cercare di migliorare | VisualizzaAndamento, SceltaParametri, ConfigurazionePortafoglio, Registrazione, Autenticazione, RimozioneAccount |
| Protezione dei dati | Sicurezza | Peggioramento nella velocità di memorizzazione e ricerca dati, ma miglioramento privacy dati memorizzati | SceltaParametri, ConfigurazionePortafoglio, Registrazione, Autenticazione, AttuazioneInvestimento, CreazioneLog |
| Protezione delle comunicazioni | Sicurezza | Peggioramento nei tempi di risposta, ma miglioramento privacy dati scambiati | VisualizzaAndamento, SceltaParametri, ConfigurazionePortafoglio, Registrazione, Autenticazione, RimozioneAccount, ResocontoMensile, AttuazioneInvestimento, VisualizzaUtente, VisualizzaLog |
| Velocità interazione | Efficienza | Cercare di migliorare | Registrazione, |

| | | | |
|---------------------|--|--|---|
| con sistemi esterni | | | AttuazioneInvestimento, AggiornaValori |
|---------------------|--|--|---|

Analisi delle interazioni

Tabella maschere

| Maschera | Informazioni | Funzionalità |
|--------------------------------|---|---|
| View Registrazione | Input per Username, Password, Indirizzo Email, Metodo di Pagamento, Moneta di Riferimento, Codice di Verifica | Registrazione |
| View Autenticazione | Username, Password | Autenticazione |
| Home VisualizzaAndamento | Grafici contenenti l'Andamento del Portafoglio dell'Utente e possibilità di applicare un filtro | VisualizzaAndamento |
| View FiltroVisualizzazione | Possibilità di scegliere Nome Moneta, Intervallo di date e/o Importo della Spesa in Valuta Fiat | VisualizzaAndamento |
| Home Configurazione | Mostra i dati se già inseriti dall'Utente e permette di navigare alle maschere di inserimento | ConfigurazionePortafoglio , SceltaParametri |
| View SceltaParametri | Input per Intervallo di Investimento e Budget. Calcolo della Previsione | SceltaParametri |
| View ConfigurazionePortafoglio | Lista di Input per inserire Nome Criptovaluta e Percentuale di Budget assegnata alla Criptovaluta | ConfigurazionePortafoglio |
| Home VisualizzaUtente | Lista di Riepilogo Ordine degli utenti, Input per scegliere un Utente | VisualizzaUtente |
| Home VisualizzaLog | Lista delle eventuali segnalazioni generate dall'analisi dei log e lista dei log | VisualizzaLog |

Tabella sistemi esterni

| Sistema | Descrizione | Protocollo di interazione | Livello di sicurezza |
|---|---|--|---|
| Piattaforma di Exchange | Servizio al quale ci si collega per effettuare Depositi e Investimenti nel Portafoglio dell'Utente | Per il dettaglio delle API consultare: https://developers.coinbase.com/api/v2 Il Metodo di Pagamento conterrà i parametri per connettersi al Portafoglio e per identificare il tipo di pagamento (vedi nota successiva) per effettuare i depositi di Valuta Fiat di Riferimento | Molto Alto. Di primaria importanza tenere al sicuro i dati del Metodo di Pagamento. |
| Piattaforma per l'invio di messaggi Email | Sarà utilizzato per l'invio di mail agli Utenti: <ul style="list-style-type: none"> • In fase di Registrazione • Per l'invio del Resoconto mensile • Per segnalare eventuali fallimenti nel Deposito | Bisogna specificare l'Indirizzo Email del destinatario (l'Utente), l'oggetto del messaggio e il corpo della mail | Media. Non vengono scambiati dati particolarmente sensibili. |

Note: Dopo un'analisi delle API offerte dalla Piattaforma di Exchange, è emerso che non sarà necessario un servizio di membership (es. Paypal) come indicato nell'abstract, bensì per effettuare i pagamenti automatici si utilizzerà il servizio già collegato all'account personale dell'Utente sulla Piattaforma. A questo proposito anche Metodo di Pagamento sarà da qui in avanti inteso come insieme di parametri per connettersi all'account personale dell'Utente sulla Piattaforma di Exchange e tipo di pagamento desiderato tra quelli già collegati al suo account.

Analisi Ruoli e Responsabilità

Tabella Ruoli

| Ruolo | Responsabilità | Maschere | Riservatezza | Numerosità |
|----------------|---|--|---|---|
| Utente | Gestisce la Distribuzione Percentuale del suo Portafoglio e i Parametri di Investimento. Visualizza e filtra l'Andamento del proprio Portafoglio e i Riepiloghi dei suoi Investimenti | View Registrazione, View Autenticazione, Home VisualizzaAndamento, View FiltroVisualizzazione, Home Configurazione, View SceltaParametri, View ConfigurazionePortafoglio | È richiesto un grado di riservatezza alto | Il numero massimo di Utenti è limitato dalle risorse del sistema |
| Amministratore | Gestisce e visualizza le segnalazioni sui log. Visualizza e filtra tutti gli Investimenti degli Utenti. Ha inoltre le stesse funzionalità dell'Utente. | Tutte | È richiesto un grado di riservatezza alto | Almeno 2-3 Amministratori per gestire al meglio i log e le segnalazioni |

Utente: Tabella Ruolo-Informazioni

| Informazione | Tipo di accesso |
|---|------------------------|
| Username | Scrittura |
| Password | Scrittura |
| Indirizzo Email | Scrittura |
| Codice di Verifica | Lettura/Scrittura |
| Riepilogo Ordine | Lettura |
| Valore Portafoglio | Lettura |
| Nome Criptovaluta | Lettura/Scrittura |
| Intervallo di Date | Scrittura |
| Importo della Spesa | Scrittura |
| Intervallo di Investimento | Lettura/Scrittura |
| Budget | Lettura/Scrittura |
| Previsione Spesa | Lettura |
| Percentuale di Budget assegnata alla Criptovaluta | Lettura/Scrittura |
| Valuta Fiat di Riferimento | Scrittura |
| Metodo di Pagamento | Scrittura |
| Resoconto | Lettura |

Amministratore: Tabella Ruolo-Informazioni

| Informazione | Tipo di accesso |
|--|------------------------|
| Username | Lettura/Scrittura |
| Data | Lettura |
| Ora | Lettura |
| Tipo Operazione | Lettura |
| Messaggio | Lettura |
| Segnalazione | Lettura |
| Derivanti dal fatto che l'Amministratore è anche un Utente: | |
| Password | Scrittura |
| Indirizzo Email | Scrittura |
| Codice di Verifica | Lettura/Scrittura |
| Riepilogo Ordine | Lettura |
| Valore Portafoglio | Lettura |
| Nome Criptovaluta | Lettura/Scrittura |
| Intervallo di Date | Scrittura |
| Importo della Spesa | Scrittura |
| Intervallo di Investimento | Lettura/Scrittura |
| Budget | Lettura/Scrittura |
| Previsione Spesa | Lettura |
| Percentuale di Budget assegnata alla Criptovaluta | Lettura/Scrittura |
| Valuta Fiat di Riferimento | Scrittura |
| Metodo di Pagamento | Scrittura |
| Resoconto | Lettura |

Scomposizione del Problema

Tabella scomposizione funzionalità

| Funzionalità | Scomposizione |
|------------------------|---|
| Registrazione | VerificaDatInseriti, GestioneCodiceVerifica, MemorizzaUtente |
| AttuazioneInvestimento | DepositoFiat, CompraCriptovaluta, CreaRiepilogo |

Registrazione: Tabella Sotto-Funzionalità

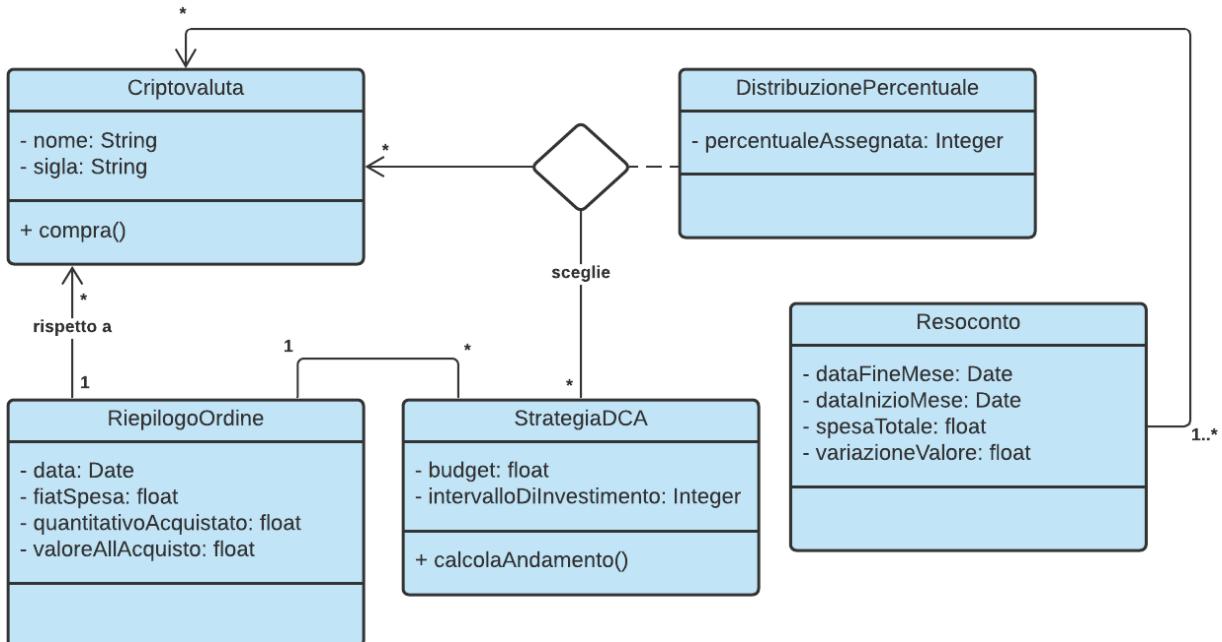
| Sotto-funzionalità | Sotto-funzionalità | Legame | Informazioni |
|----------------------------|----------------------------|--|--|
| GestioneCodiceVe rifica | VerificaDatInseriti | Il codice di verifica non viene inviato finché non vengono inseriti e validati tutti i dati dell'Utente | Username, Password, Indirizzo Email, Metodo di Pagamento, Valuta di Riferimento, Codice di Verifica |
| MemorizzaUtente | GestioneCodiceVe rifica | Non si può registrare l'Utente nel sistema finché questo non inserisce il Codice di Verifica corretto | Username, Password, Indirizzo Email, Metodo di Pagamento, Valuta di Riferimento, Codice di Verifica |

AttuazioneInvestimento: Tabella Sotto-Funzionalità

| Sotto-funzionalità | Sotto-funzionalità | Legame | Informazioni |
|--------------------|--------------------|--|--|
| CompraCriptovaluta | DepositoFiat | Non si possono comprare Criptovalute senza aver effettuato il Deposito di Valuta Fiat sul Portafoglio | Metodo di Pagamento, Budget, Nome Criptovaluta, Percentuale di Budget assegnata alla Criptovaluta |
| CreaRiepilogo | CompraCriptovaluta | Non si può creare il Riepilogo Ordine senza aver completato l'Ordine | Riepilogo Ordine |

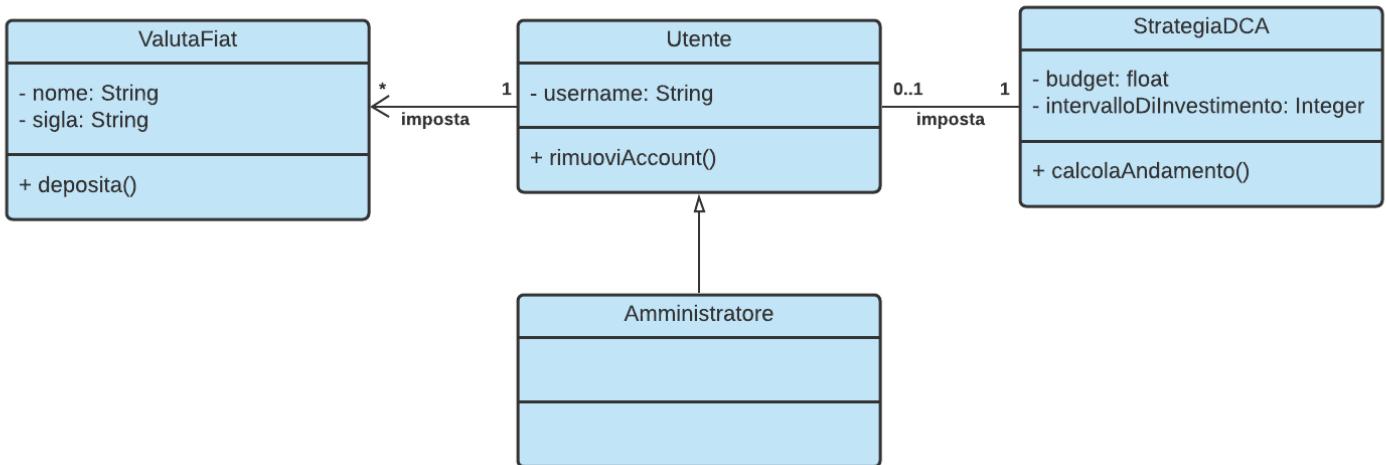
Modello del dominio

Di seguito è riportata la parte del Modello del Dominio relativa alla gestione degli Investimenti e configurazione della Strategia di DCA dell'Utente.

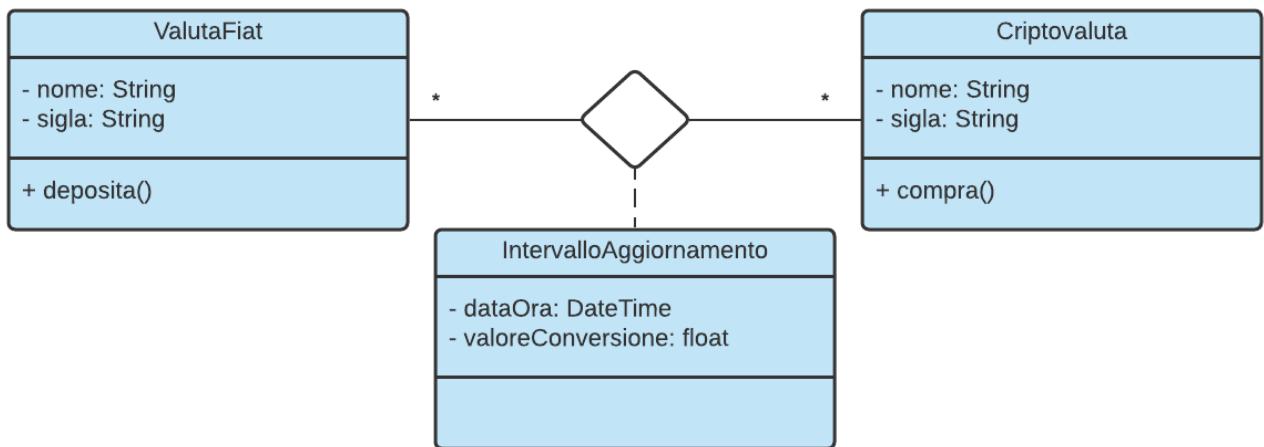


Vincolo: Non è possibile produrre un **RiepilogoOrdine** fino a quando non sono stati impostati gli attributi `budget`, `intervalloDiInvestimento` ed una **DistribuzionePercentuale**.

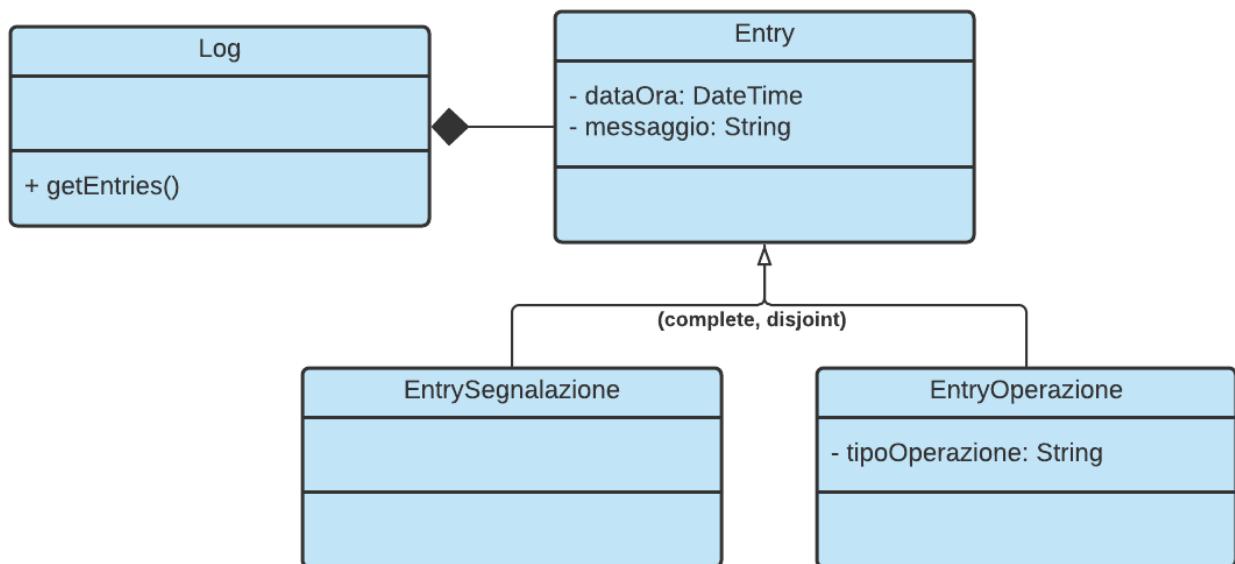
Di seguito viene invece riportata la parte di Modello del Dominio relativa all'Utente e all'impostazione della sua Valuta Fiat di Riferimento.



Il seguente diagramma delle classi rappresenta la relazione presente tra le Criptovalute e le Valute Fiat, utilizzata per calcolare il valore di una rispetto all'altra (e viceversa).



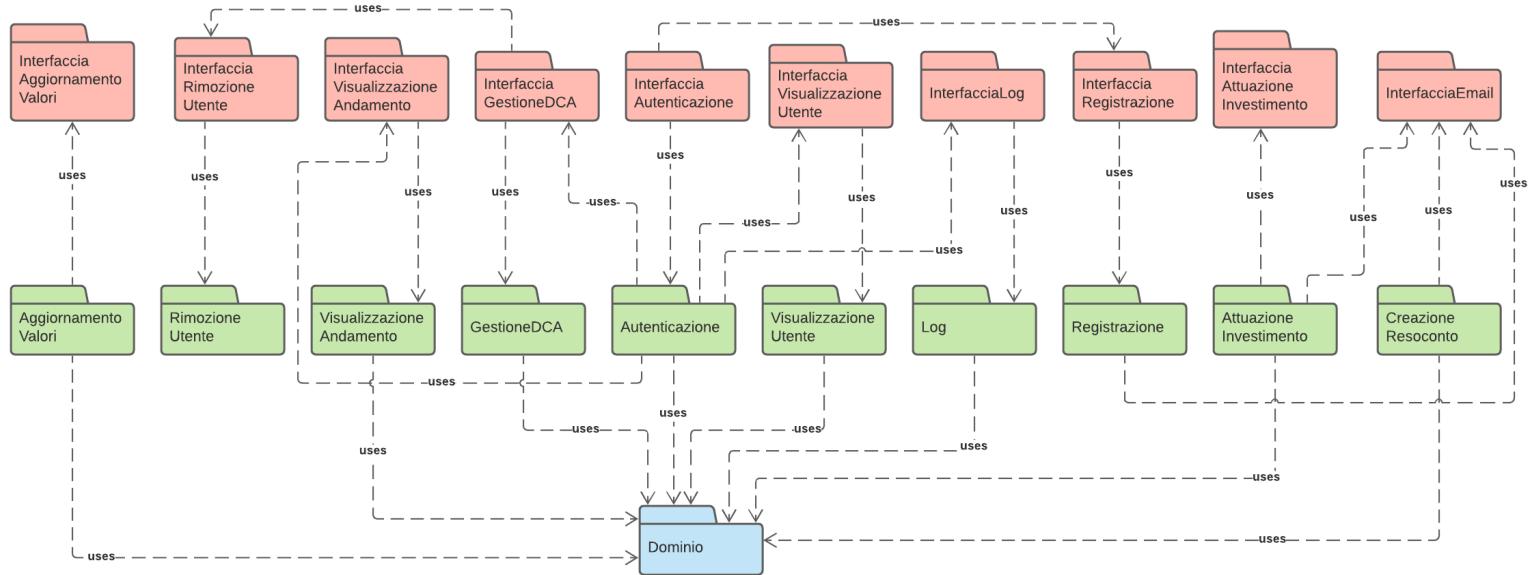
Il seguente diagramma delle classi rappresenta infine la parte relativa alla gestione dei Log.



Architettura logica: struttura

Diagramma dei package

Di seguito la rappresentazione del diagramma dei package secondo il pattern BCE.



Note:

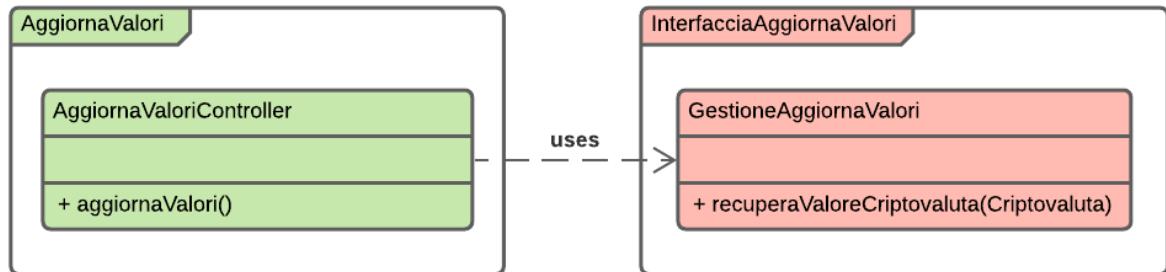
- L'Autenticazione utilizza il dominio perché in base ai parametri impostati dall'utente nella sua StrategiaDCA vengono visualizzate Home differenti (vedi Diagramma di sequenza dell' Autenticazione).
- Inoltre le relazioni tra interfacce servono per evidenziare la navigabilità tra le stesse e permettere la loro raggiungibilità.

Diagramma delle classi: Dominio

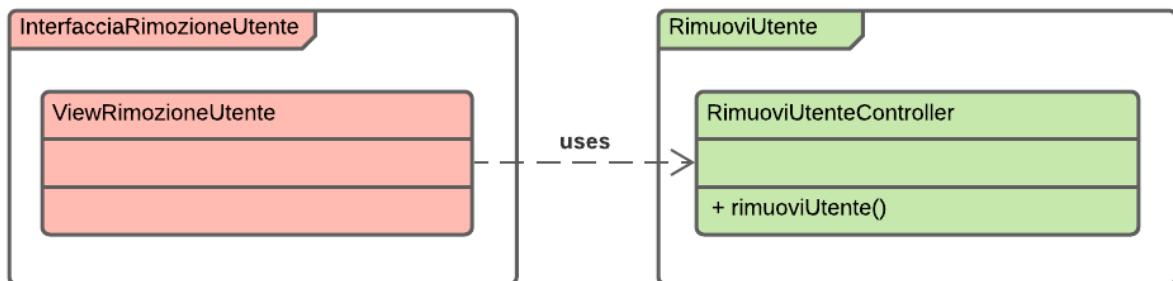
Il diagramma delle classi relativa alla parte di dominio viene omesso in quanto riportato in precedenza.

Diagramma delle classi: Controller & Interfacce

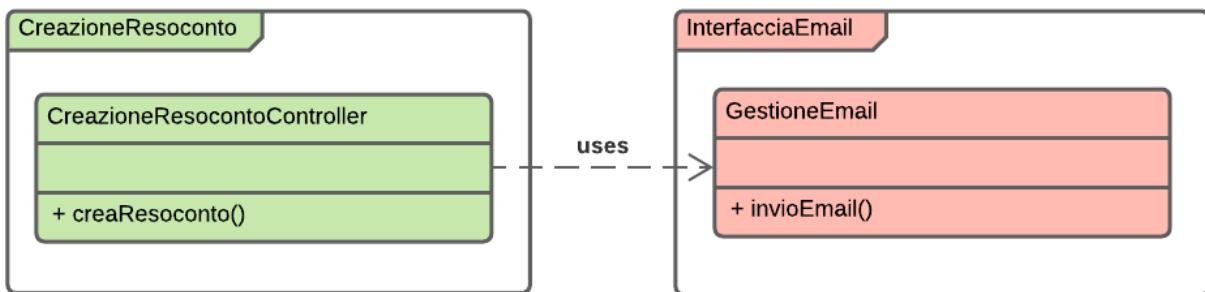
AggiornaValori & InterfacciaAggiornaValori



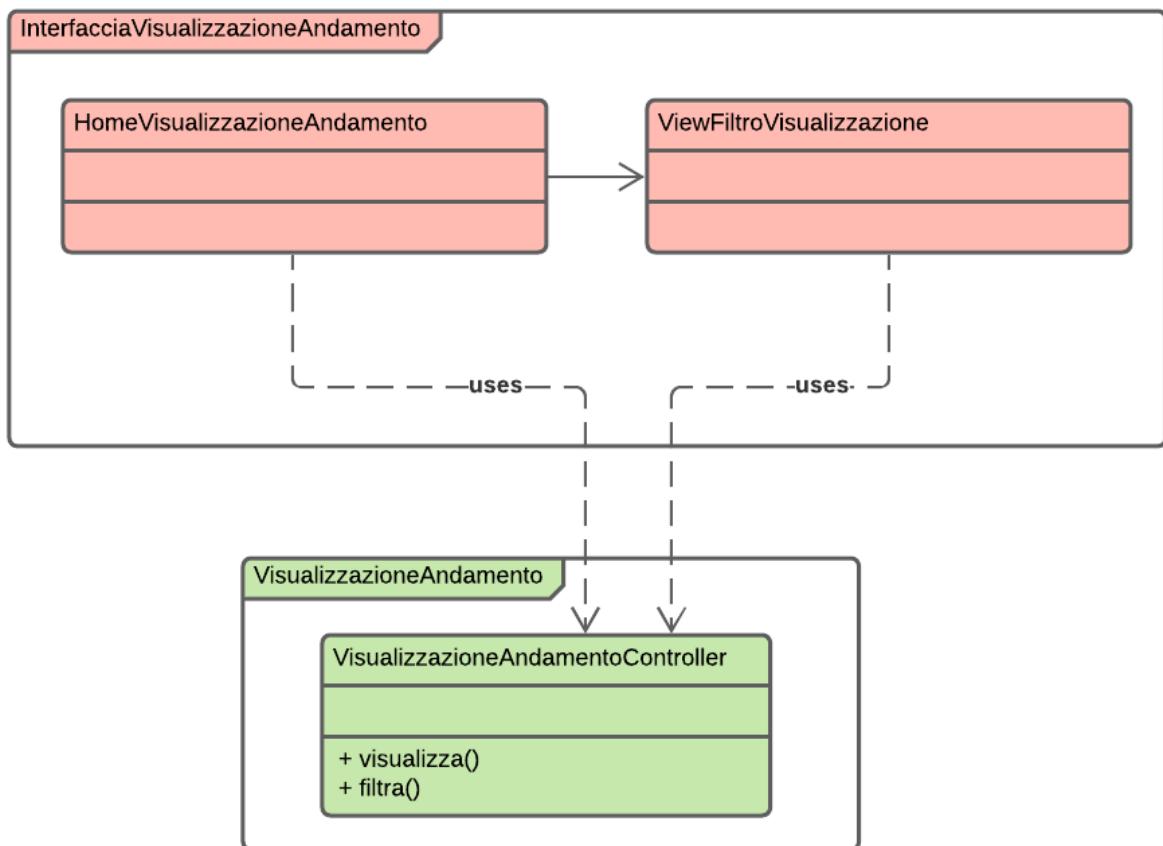
RimuoviUtente & InterfacciaRimozioneUtente



CreazioneResoconto & InterfacciaEmail

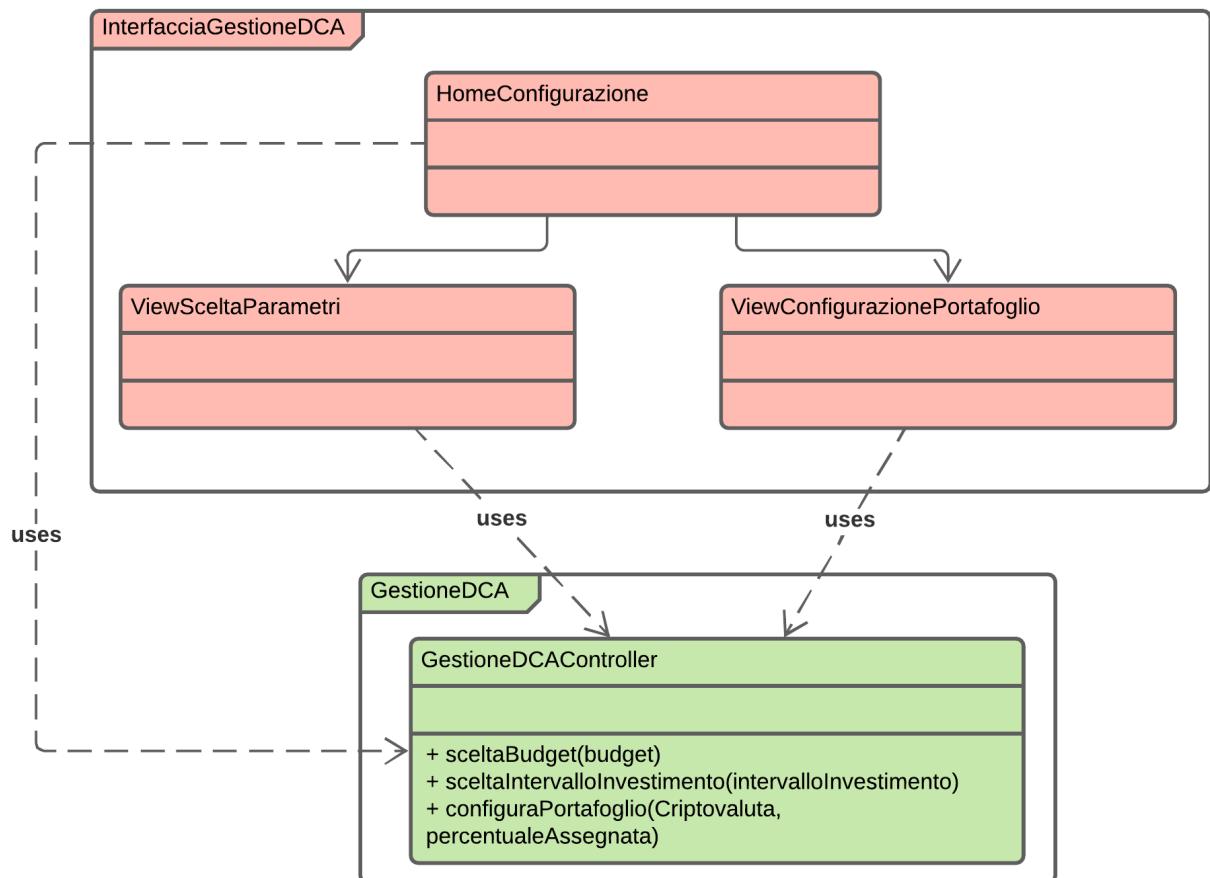


VisualizzazioneAndamento & InterfacciaVisualizzazioneAndamento

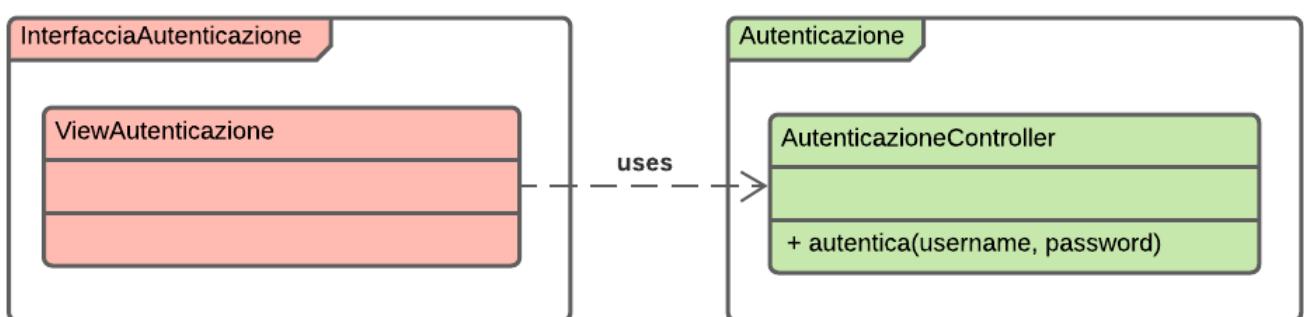


GestioneDCA & InterfacciaGestioneDCA

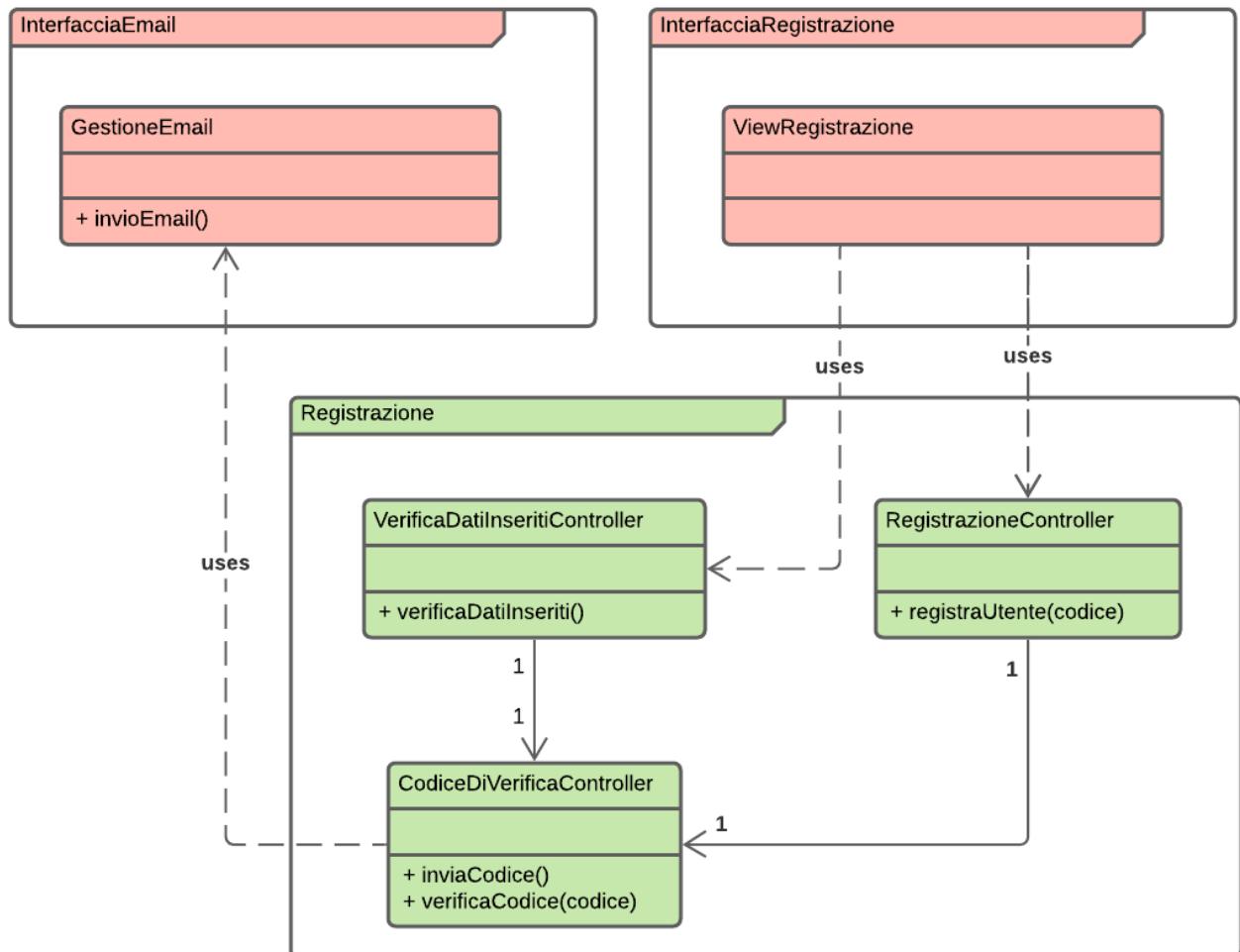
Il metodo *configuraPortafoglio* serve per aggiungere o modificare la Percentuale di Budget Assegnata ad una Criptovaluta, nella Distribuzione Percentuale dell'Utente



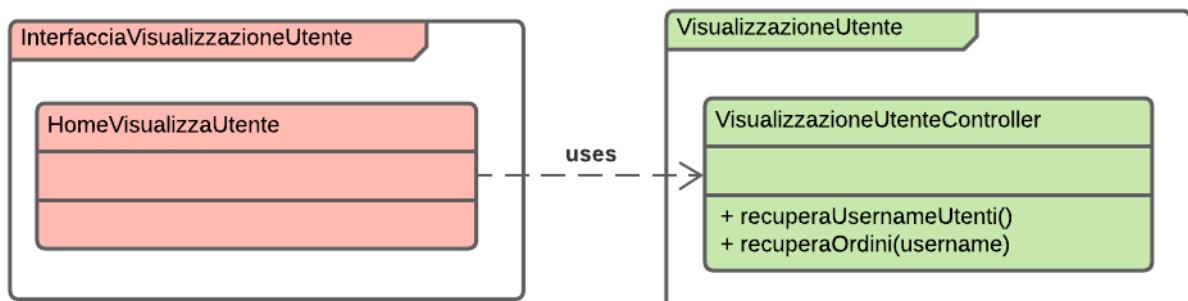
Autenticazione & InterfacciaAutenticazione



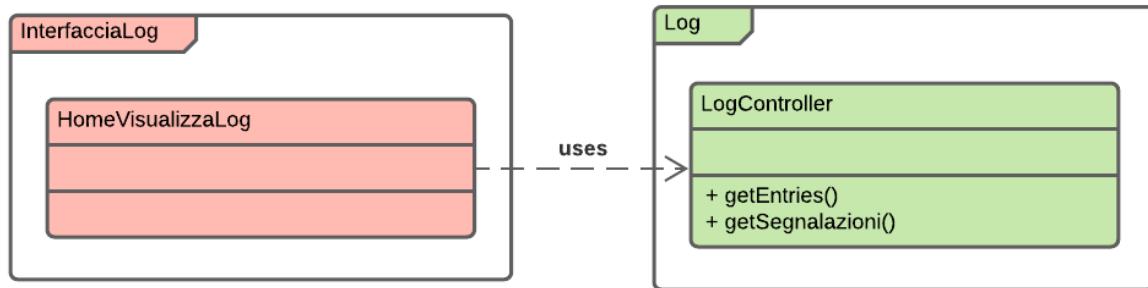
Registrazione & InterfacciaRegistrazione & InterfacciaEmail



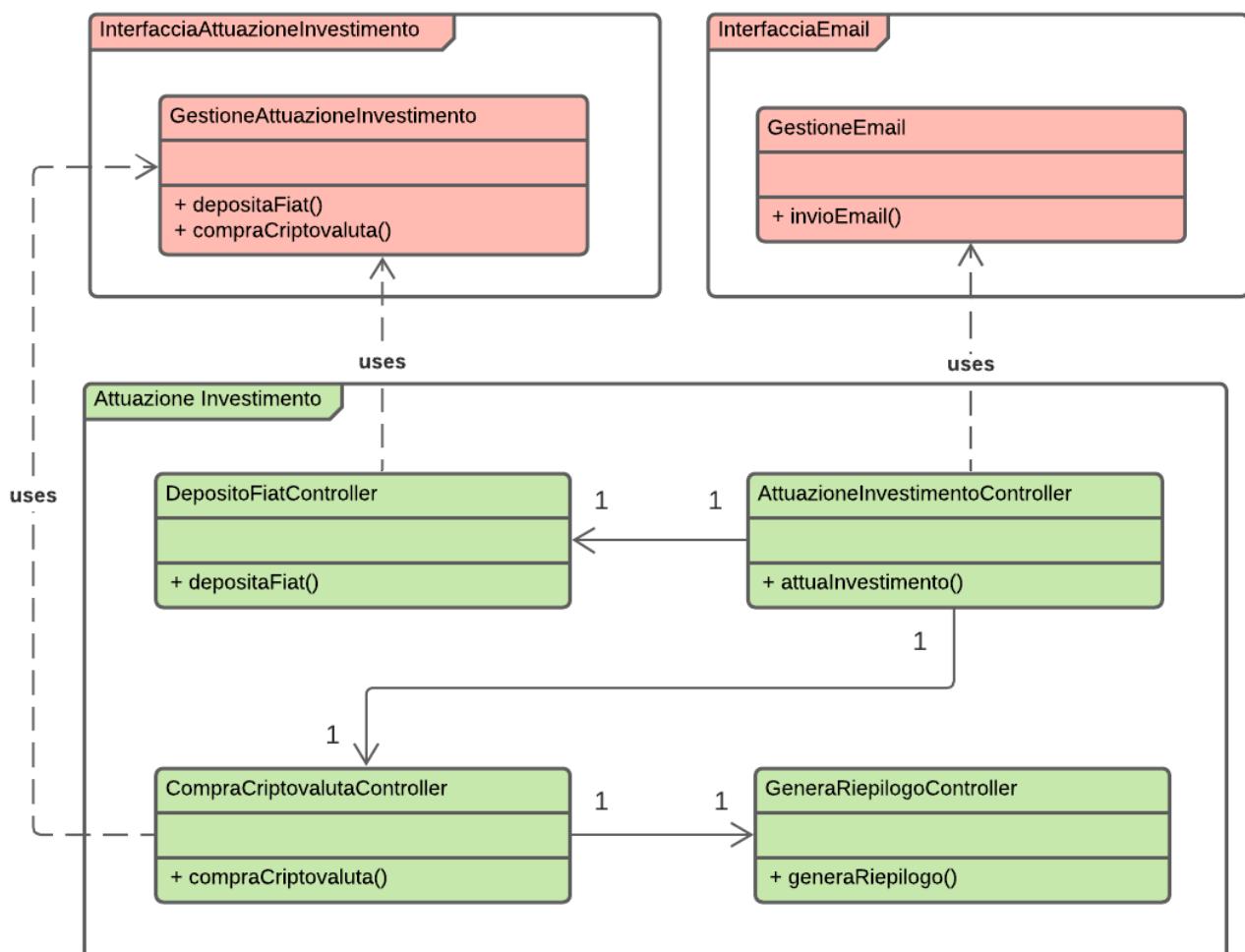
VisualizzazioneUtente & InterfacciaVisualizzazioneUtente



Log & InterfacciaLog



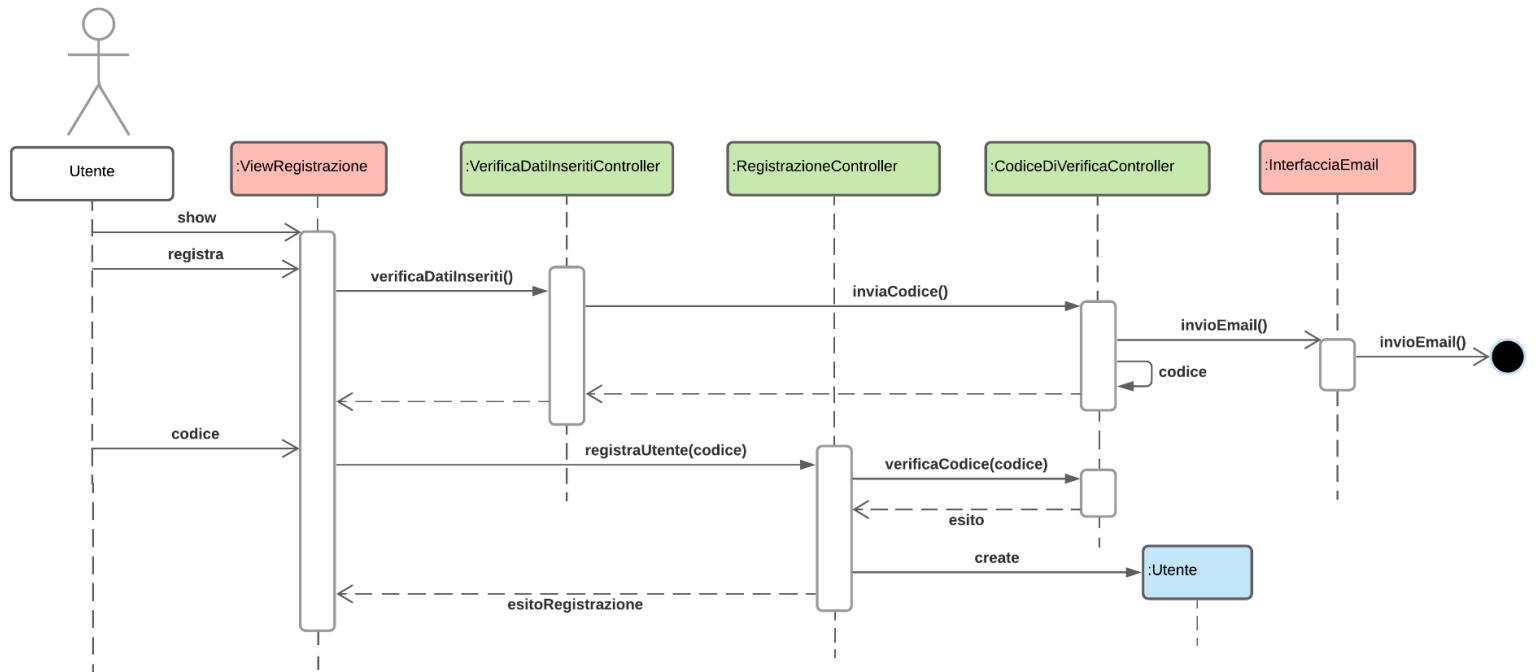
AttuazioneInvestimento & InterfacciaAttuazioneInvestimento & InterfacciaEmail



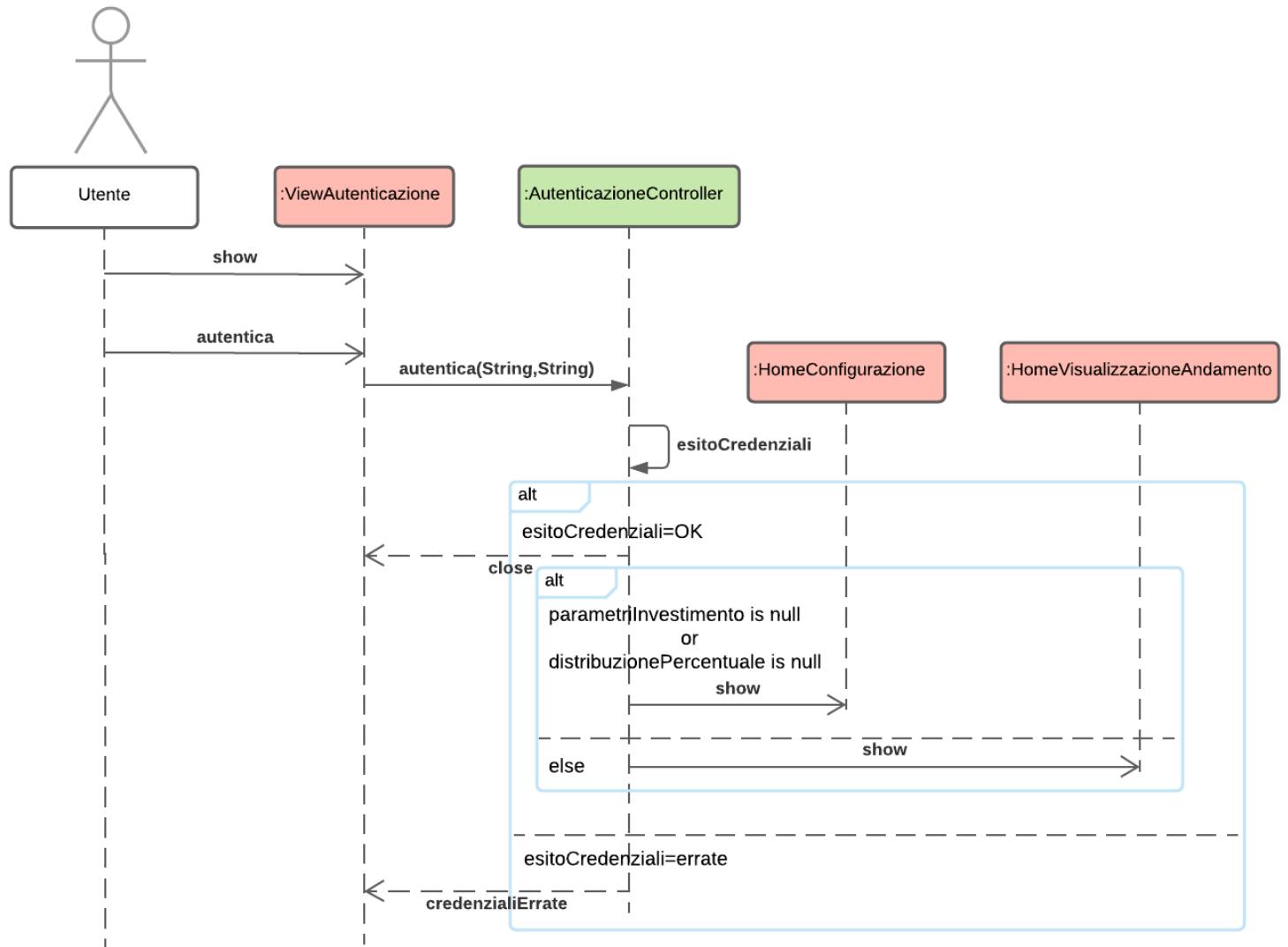
Architettura logica: interazione

Diagrammi di sequenza

Registrazione

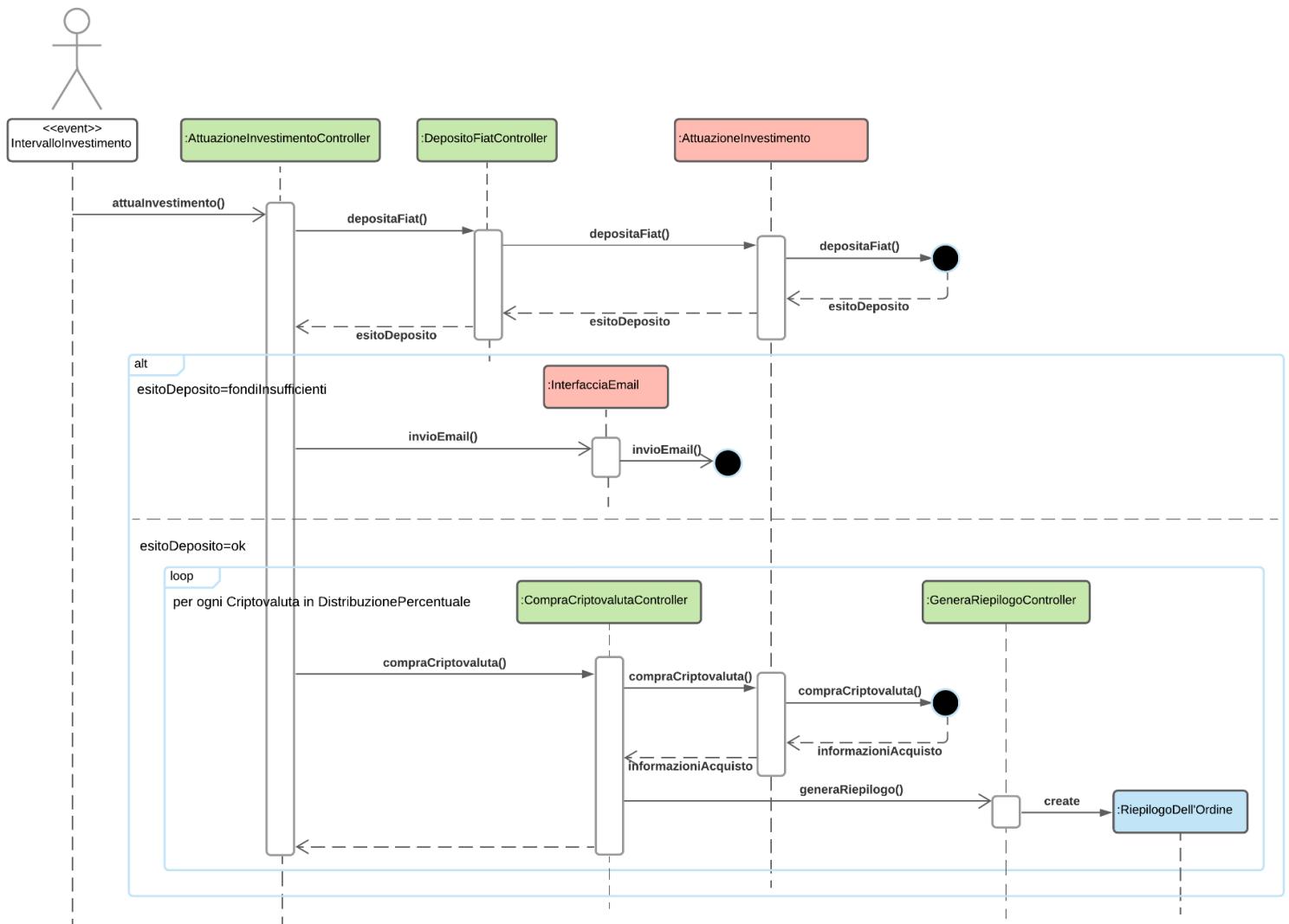


Autenticazione



Per non compromettere eccessivamente la leggibilità del diagramma, si è deciso di omettere le barre relative al tempo di attivazione delle entità.
Le modalità con cui i Parametri di Investimento e la Distribuzione Percentuale verranno recuperati saranno indicate nel Documento di Progettazione.

AttuazioneInvestimento



Diagrammi di Stato/Attività

Dopo aver analizzato in maniera approfondita il comportamento delle entità presenti nel progetto all'evolversi del loro stato e dello svolgimento delle attività, aver richiesto un ricevimento ed aver avuto un confronto con il professore Marco Patella e il tutor Kevin Michael Frick abbiamo concluso che non è necessario riportare i diagrammi di stato e/o attività di alcuna entità.

Piano di lavoro

| Package | Progetto | Sviluppo |
|-------------------------------------|---------------------------|---------------------------|
| Dominio | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| AggiornamentoValori | Donati, Taddei, Tamagnini | Donati, Taddei |
| RimozioneUtente | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| VisualizzazioneAndamento | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| GestioneDCA | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| Autenticazione | Donati, Taddei, Tamagnini | Donati |
| Registrazione | Donati, Taddei, Tamagnini | Donati |
| VisualizzazioneUtente | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| Log | Donati, Taddei, Tamagnini | Tamagnini |
| AttuazioneInvestimento | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| CreazioneResoconto | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| InterfacciaAggiornamentoValori | Donati, Taddei, Tamagnini | Taddei |
| InterfacciaRimozioneUtente | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| InterfacciaVisualizzazioneAndamento | Donati, Taddei, Tamagnini | Taddei, Tamagnini |
| InterfacciaGestioneDCA | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| InterfacciaAutenticazione | Donati, Taddei, Tamagnini | Donati |

| | | |
|-----------------------------------|------------------------------|------------------------------|
| InterfacciaRegistrazione | Donati, Taddei, Tamagnini | Donati |
| InterfacciaVisualizzazioneUtente | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |
| InterfacciaLog | Donati, Taddei, Tamagnini | Tamagnini |
| InterfacciaAttuazioneInvestimento | Donati, Taddei, Tamagnini | Taddei |
| InterfacciaEmail | Donati, Taddei, Tamagnini | Donati, Taddei, Tamagnini |

Prototipo

Nel prototipo che verrà sviluppato si darà la possibilità di registrarsi e autenticarsi, impostare i parametri per l'investimento e visualizzare gli acquisti già effettuati dal sistema.

I tempi di rilascio previsti sono i seguenti:

- Progettazione conclusa entro il 30/05/2021
- Sviluppo del prototipo entro 20 giorni dalla data di consegna della documentazione relativa alla progettazione
- Sviluppo delle singole parti con collaudo unitario entro un mese rispetto al fine della progettazione
- Integrazione e test dell'intero sistema entro 2 settimane rispetto alla fine dello sviluppo

Sviluppi Futuri

- Possibilità per l'Utente di effettuare Investimenti in tempo reale direttamente dal sistema
- Dare la possibilità agli Utenti di configurare più Strategie DCA
- Modalità di Attuazione dell'Investimento più strategica, effettuata in momenti in cui il mercato è favorevole

Piano del collaudo

Di seguito vengono riportati i test di alcune delle classi del dominio realizzati mediante JUnit.

```
public class TestEntry
{
    private EntryOperazione entryOperazione;
    private EntrySegnalazione entrySegnalazione;

    @BeforeEach
    public void entrySetup()
    {
        entryOperazione = new EntryOperazione(LocalDateTime.of(2021, 05, 02, 17,
            47, 13), "Password errata, Utente: user1", "Autenticazione");
        entrySegnalazione = new EntrySegnalazione(LocalDateTime.of(2021, 05, 02,
            17, 47, 20), "Rilevato tentativo di accesso a Utente: user1");
    }

    @Test
    public void testEntryOperazione()
    {
        assertTrue(entryOperazione instanceof Entry);
        assertTrue(entryOperazione instanceof EntryOperazione);
        assertEquals(entryOperazione.getDataOra(), LocalDateTime.of(2021, 05,
            02, 17, 47, 13));
        assertEquals(entryOperazione.getMessaggio(), "Password errata, Utente:
            user1");
        assertEquals(entryOperazione.getTipoOperazione(), "Autenticazione");
    }

    @Test
    public void testEntrySegnalazione()
    {
        assertTrue(entrySegnalazione instanceof Entry);
        assertTrue(entrySegnalazione instanceof EntrySegnalazione);
        assertEquals(entrySegnalazione.getDataOra(), LocalDateTime.of(2021, 05,
            02, 17, 47, 20));
        assertEquals(entrySegnalazione.getMessaggio(), "Rilevato tentativo di
            accesso a Utente: user1");
    }
}
```

```
public class TestIntervalloAggiornamento
{
    private IntervalloAggiornamento intervalloAggiornamento;

    @BeforeEach
    public void intervalloAggiornamentoSetup()
    {
        intervalloAggiornamento = new
            IntervalloAggiornamento(LocalDateTime.of(2020, 05, 02, 17, 8,
                12), 1.21f, "EUR", "ADA");
    }

    @Test
    public void testGetterIntervalloAggiornamento()
    {
        assertEquals(intervalloAggiornamento.getDataOra(),
            LocalDateTime.of(2020, 05, 02, 17, 8, 12));
        assertEquals(intervalloAggiornamento.getValoreConversione(), 1.21f);
        assertEquals(intervalloAggiornamento.getSiglaValutaFiat(), "EUR");
        assertEquals(intervalloAggiornamento.getSiglaCriptovaluta(), "ADA");
    }
}
```

Progettazione

Progettazione architetturale

Requisiti non funzionali

Dalla tabella dei requisiti non funzionali sono emersi in particolare:

- Velocità di Memorizzazione e Recupero dati
- Usabilità delle Maschere
- Disponibilità
- Latenze Basse nell'aggiornamento dei valori dai sistemi esterni
- Protezione dei dati
- Protezione delle comunicazioni

Per quanto riguarda la Velocità di Memorizzazione e Recupero dati, riteniamo più importante garantire rapidità per il Recupero, rispetto alla Memorizzazione, per assicurare all'utente velocità nel caricamento e visualizzazione del grafico e dello storico delle transazioni per migliorare la fluidità durante l'utilizzo del sistema.

Per lo stesso fine riteniamo importante l'Usabilità delle Maschere, che devono essere intuitive da usare e, al contempo, essere chiare poiché tramite le Maschere l'utente configura il modo in cui le proprie risorse economiche saranno gestite.

Relativamente alla Disponibilità, è fondamentale garantire agli utenti il servizio di attuazione degli investimenti per applicare la strategia DCA, il quale comunque dipende anche dalla disponibilità della piattaforma di exchange.

Le Latenze Basse dipenderanno dalla tipologia di connessione che verrà utilizzata sul server, occorrerà dunque fornire un'adeguata larghezza di banda.

È fondamentale garantire la Protezione dei dati sul sistema, in particolar modo per i dati relativi alle chiavi utilizzate per la connessione al portafoglio esterno dell'utente.

È importante anche mantenere la Protezione delle comunicazioni, sia nelle fasi di interazioni con l'utente che nelle fasi di interazione con i sistemi esterni.

Effettuando un'analisi completa di tutti i requisiti che sono emersi riteniamo opportuno concentrarci principalmente sul garantire la Protezione di dati e comunicazioni, anche a discapito di velocità delle interazioni e recupero dei dati, dato che il sistema è a contatto con i dati economici degli utenti.

Si cerca di mantenere comunque una buona usabilità e rapidità di risposta nelle maschere che non necessitano dell'utilizzo di questi dati (es. visualizzazione degli andamenti).

Scelta dell'architettura

L'architettura più adeguata per la nostra applicazione è l'**architettura client/server a 3 livelli**.

L1 - Client

Per rispettare il vincolo del “minimo privilegio” si è deciso di disaccoppiare le funzionalità accessibili dall’Amministratore da quelle dell’Utente sviluppando due client diversi.

- Un client per le funzionalità dell’Utente.
- Un client per le funzionalità dell’Amministratore.

L2 - Server

Per il server, invece, si è deciso di adottare server diversi sulla base dell’ambito delle funzionalità:

- Un server per le funzionalità relative alla gestione dell’account dell’Utente.
- Un server per le funzionalità di Gestione e Visualizzazione degli Andamenti.
- Un server per la gestione dell’interazione con la Piattaforma di Exchange.
- Un server per i Log.

L3 - Persistenza

Per quanto riguarda la persistenza, sarà presente un server sul quale verrà installato un DBMS che gestirà i dati del sistema. Sarà poi importante la presenza di un altro server sul quale verranno memorizzati i log. Questa divisione permetterà di garantire una maggiore resistenza in caso di un’eventuale compromissione di uno dei due. Tramite un apposito meccanismo di backup, inoltre, dovrà essere garantito il ripristino del database e dei log in caso di problemi.

Le strategie di accesso e scrittura al database saranno basate su tecniche di forza bruta attraverso i metodi CRUD.

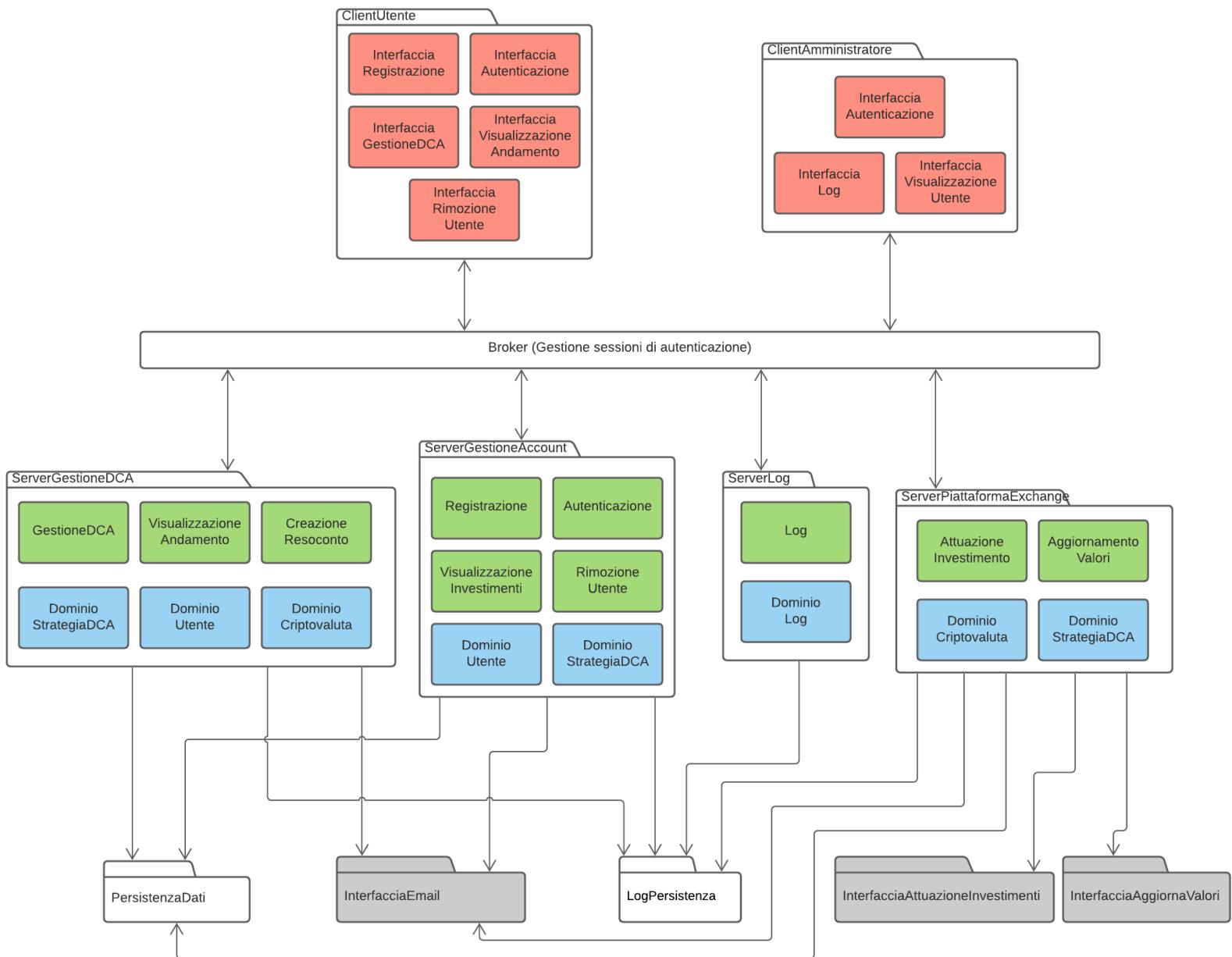
All’architettura si è deciso di aggiungere un Broker, utile per gestire la sessione di autenticazione tra tutte le funzionalità che la richiedono. Questo tipo di pattern, dato il livello di disaccoppiamento che introduce tra client e server, può facilitare l’aggiunta e l’implementazione di nuove funzionalità.

Scelte tecnologiche

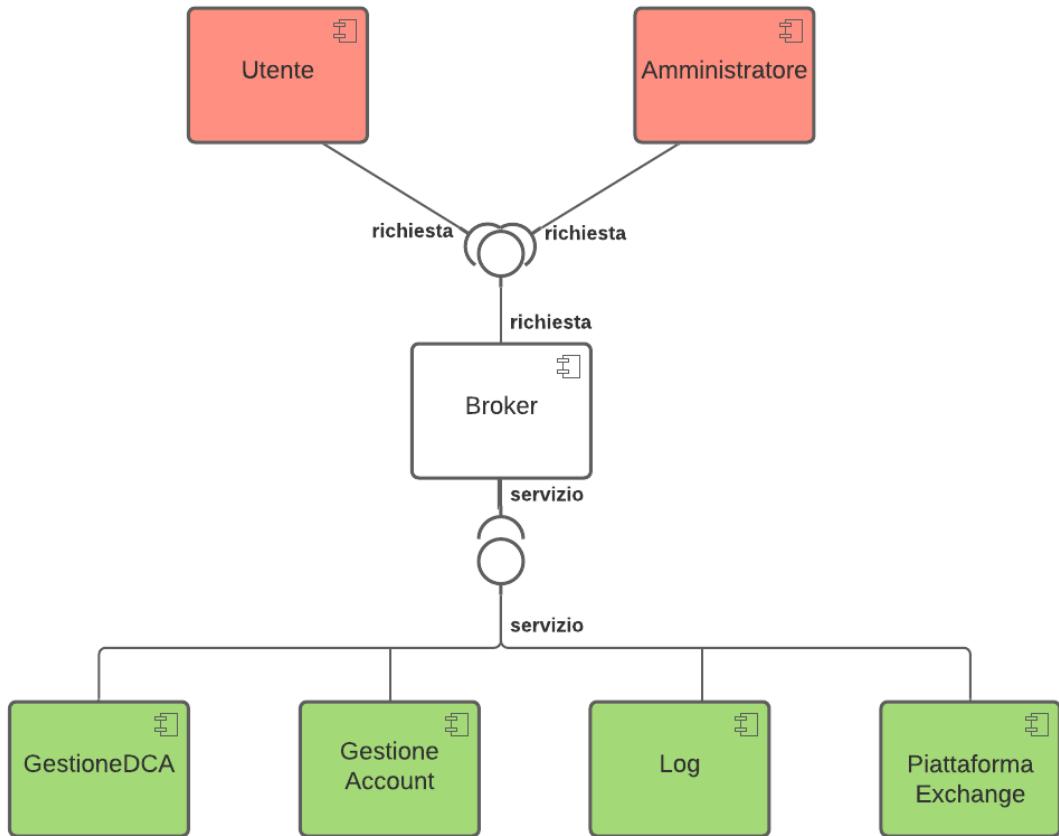
Si è deciso di sviluppare un’applicazione basata sulle tecnologie e standard del web, che garantiscono una più facile distribuzione e raggiungibilità del sistema da parte di utenti esterni. Questa facile raggiungibilità da parte di una ampia base di utenti comporta però una maggior probabilità di essere presi di mira ed attaccati da utenti malevoli.

Ovviamente l’architettura presuppone che i client siano serviti agli utenti direttamente dai server.

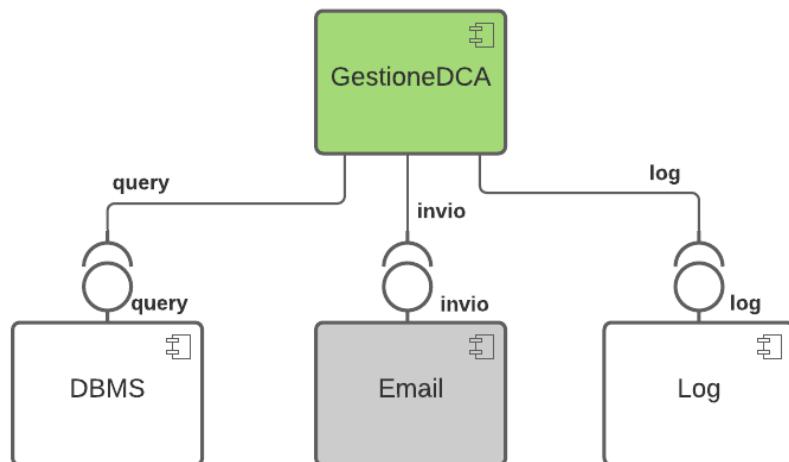
Di seguito è riportata una figura che rappresenta il diagramma dei package relativo all'Architettura del Sistema.



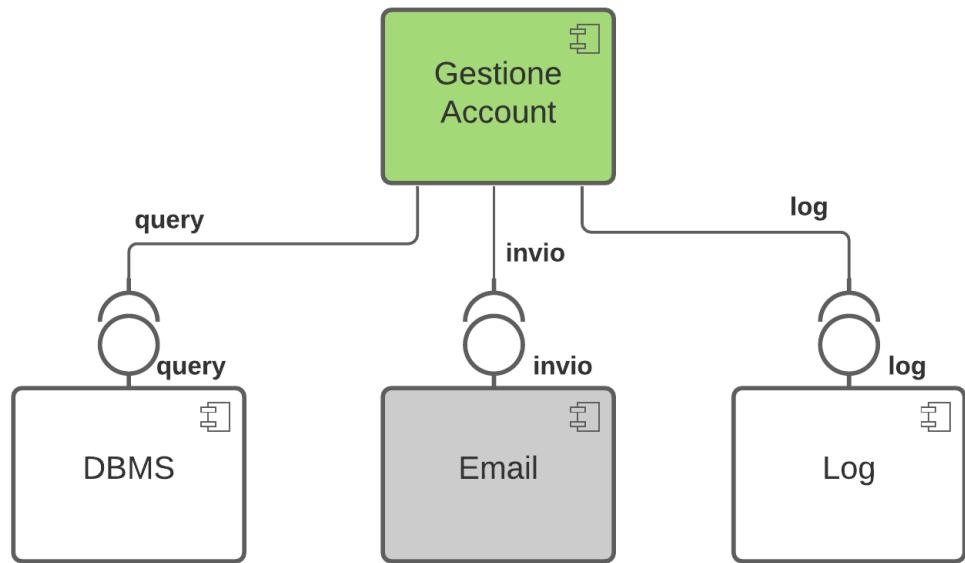
Di seguito viene invece riportata la parte di diagramma dei componenti relativa al legame tra client, broker e server. Per ogni server verrà poi analizzato il legame con persistenza e interfacce verso l'esterno.



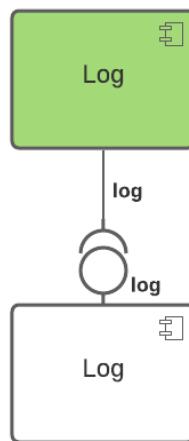
Di seguito è riportata la parte inherente al server GestioneDCA.



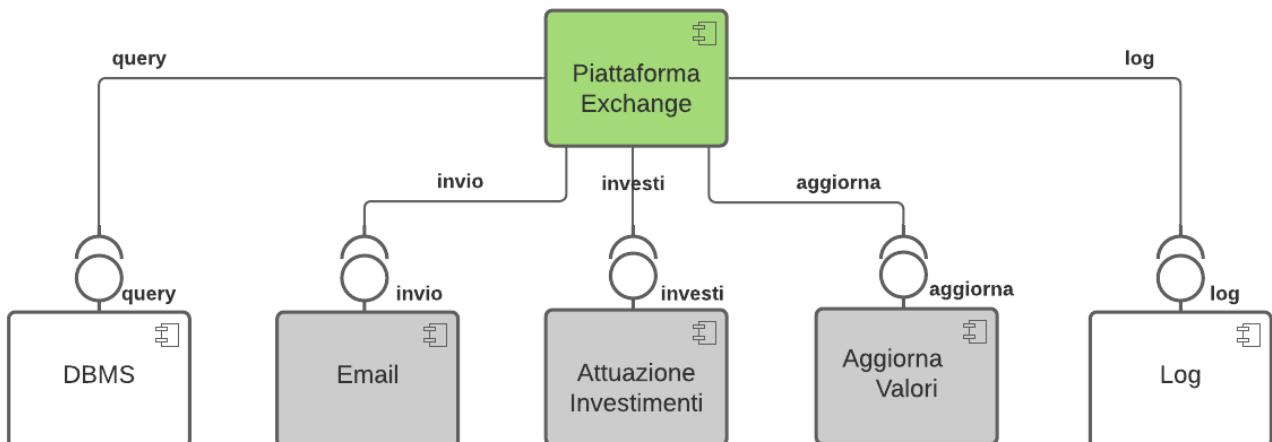
Di seguito viene invece riportata la parte inerente al server GestioneAccount.



Segue la parte relativa al server Log.



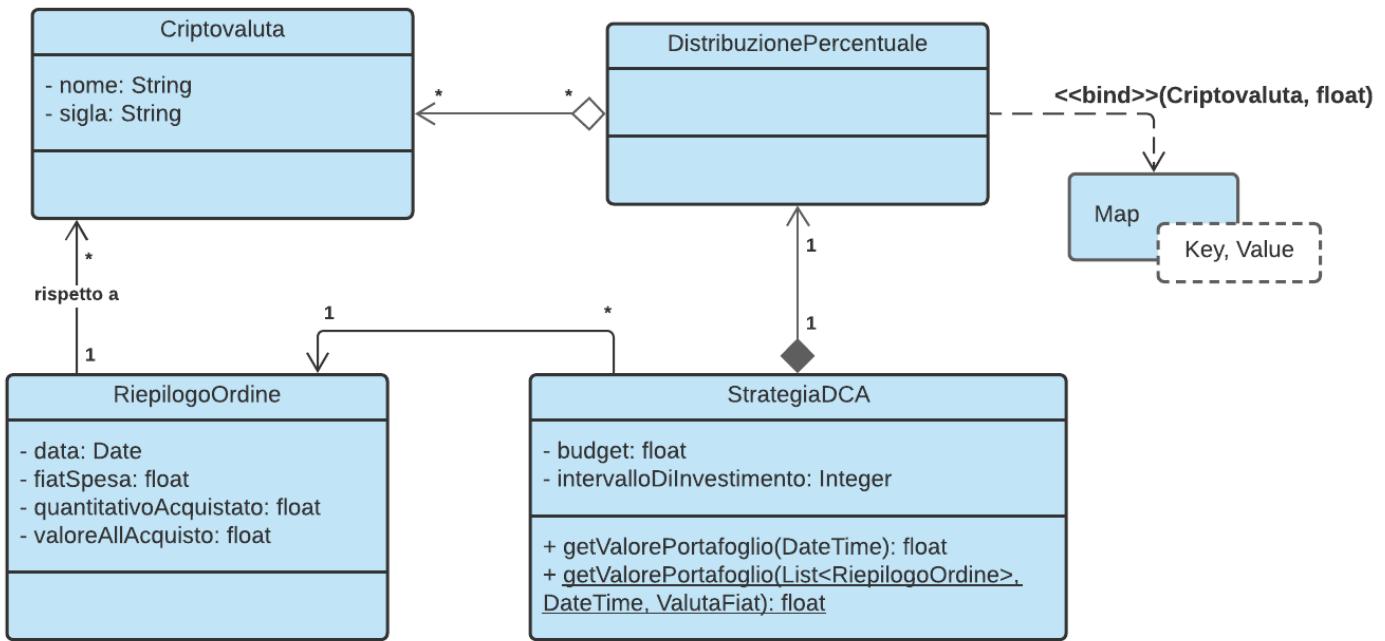
Per finire sono riportate le relazioni del server PiattaformaExchange.



Progettazione di dettaglio: Struttura

Diagramma di dettaglio: Dominio

Gestione Investimenti e Strategia DCA



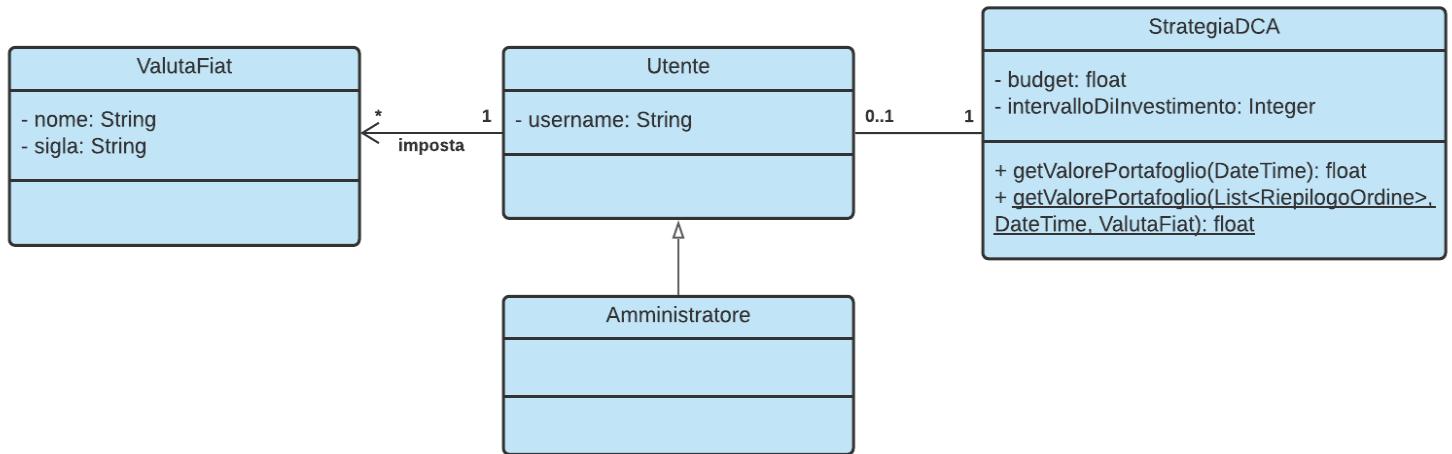
La classe *Resoconto* è stata rimossa perché non è necessario istanziarla ed utilizzarla nel sistema; sarà rappresentata da dei dati che non vengono memorizzati dopo essere stati inseriti ed inviati con una mail.

Nella classe *StrategiaDCA* sono stati inseriti i metodi per l'ottenimento del valore degli investimenti effettuati nel portafoglio dell'Utente, utilizzati nel calcolo dell'andamento, che sostituiscono il metodo *calcolaAndamento* presente in analisi:

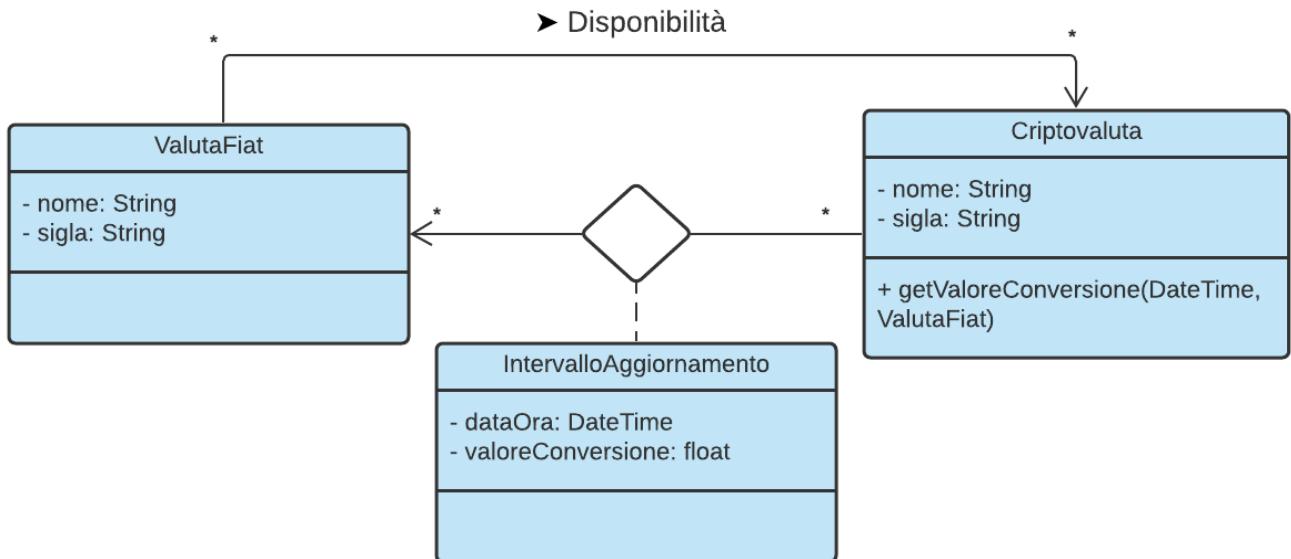
- `getValorePortafoglio(DateTime)` → Restituisce il valore complessivo, rispetto alla *ValutaFiat* di Riferimento dell'Utente, degli acquisti effettuati fino ad un certo istante di tempo passato come parametro.
- `getValorePortafoglio(List<RiepilogoOrdine>, DateTime, ValutaFiat)` → Metodo statico utilizzato per calcolare il valore monetario fino ad un dato istante di tempo rispetto ad un elenco di *RiepilogoOrdine* e una *ValutaFiat* arbitrari.

È stata inoltre tradotta la relazione *DistribuzionePercentuale* come mappa per fare in modo che ad ogni *Criptovaluta* in *StrategiaDCA* corrisponda una percentuale scelta dall'Utente, rappresentata mediante un tipo *float* per maggiore precisione.

Gestione Utente, Amministratore e Valuta Fiat di Riferimento



Gestione Aggiornamento Valori Criptovalute

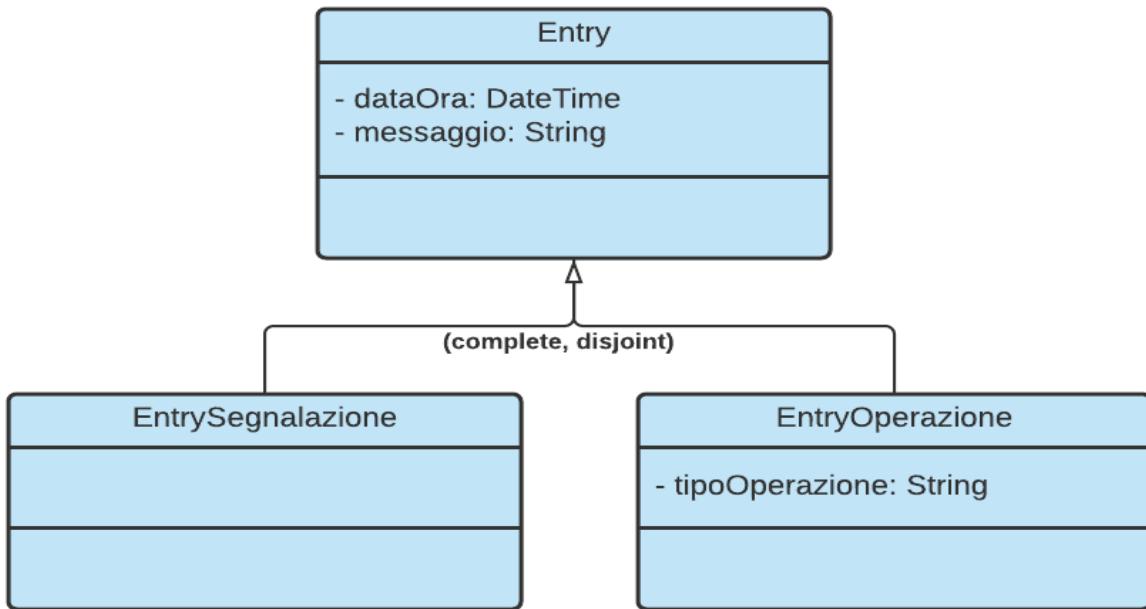


È stata aggiunta una relazione di *Disponibilità* per facilitare la ricerca delle *Criptovalute* disponibili per una certa *ValutaFiat* di Riferimento.

Ovviamente è facilmente deducibile che ogni *Criptovaluta* che ha almeno un *IntervalloAggiornamento* relativo a una *ValutaFiat* deve essere disponibile per quella *ValutaFiat*; allo stesso tempo non può essere disponibile, per una *ValutaFiat*, una *Criptovaluta* che non ha almeno un *IntervalloAggiornamento* relativo alla *ValutaFiat* stessa.

Il metodo `getValoreConversione` sarà utilizzato per ricavare il *valoreConversione* di una *Criptovaluta* rispetto ad una *ValutaFiat* in un dato istante di tempo *DateTime*.

Gestione Log

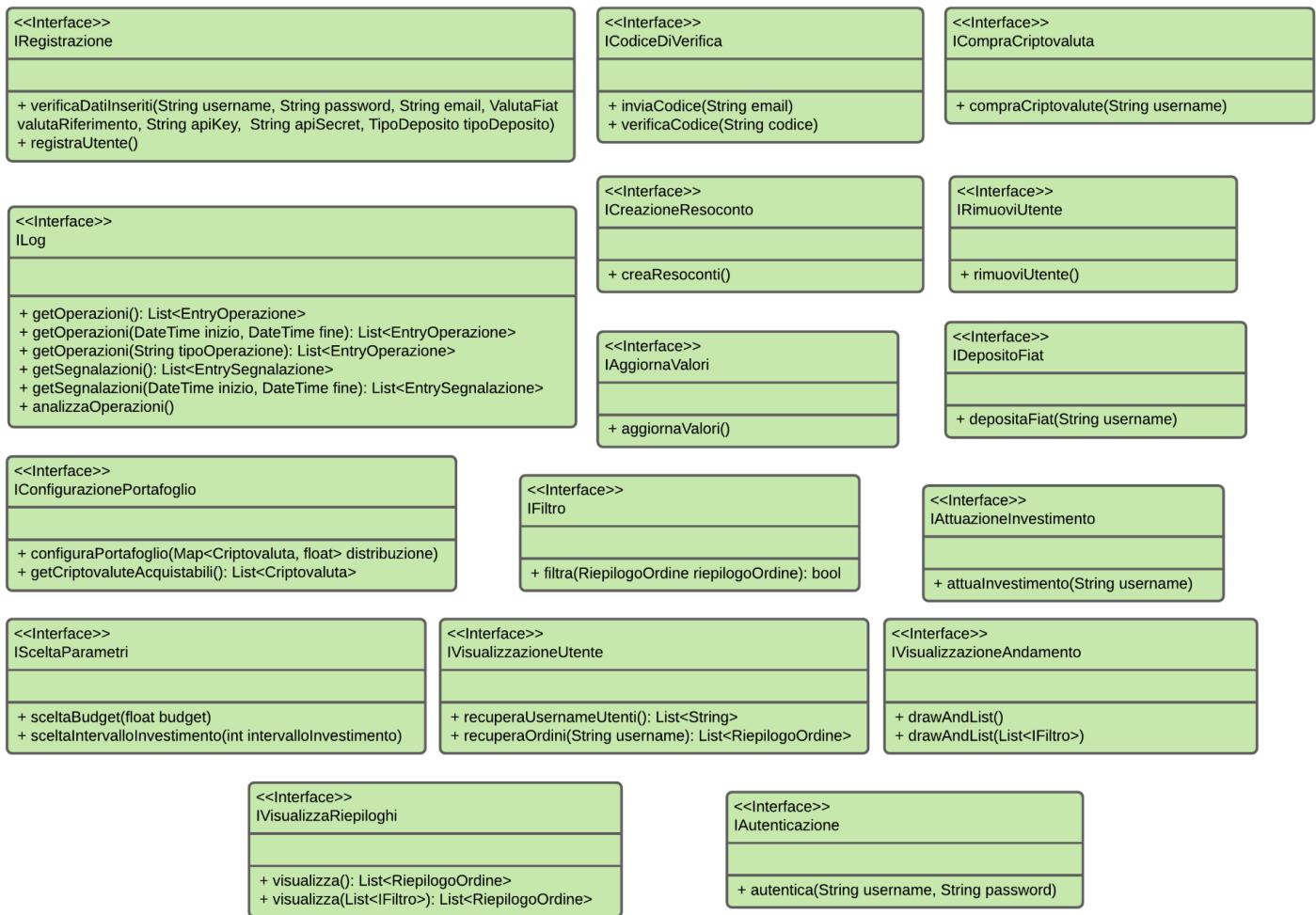


È stata inoltre rimossa la classe *Log* perché non necessaria una sua istanza all'interno del sistema, ma è facilmente rappresentabile da una lista di *Entry*.

EntrySegnalazione ed *EntryOperazione* sono disgiunte in quanto una *EntrySegnalazione* viene prodotta in seguito al riscontro di anomalie tra le *EntryOperazione*.

Un *EntryOperazione* non sarà mai un *EntrySegnalazione*.

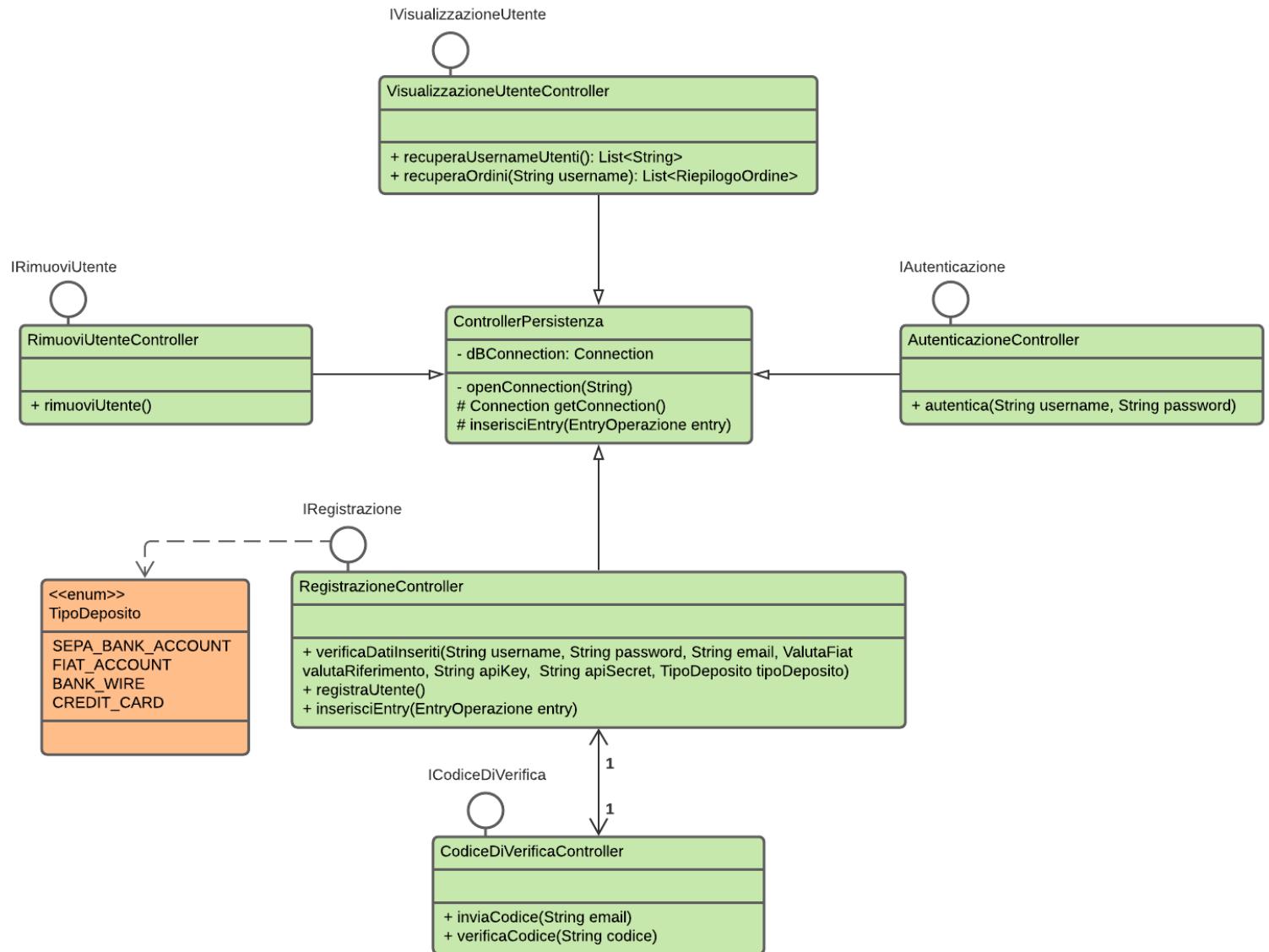
Diagramma di dettaglio: Interfacce nei server



Grazie all'utilizzo di queste interfacce sarà possibile applicare il Principio di Inversione delle Dipendenze, svincolando e nascondendo l'implementazione dei servizi offerti ai clienti mediante una dipendenza da sole astrazioni.

Diagramma di dettaglio: Controller

Gestione Utente



ControllerPersistenza è utilizzato come classe base, implementata da tutti i controller, per la gestione della connessione al DBMS e la scrittura sui log.

VisualizzazioneUtenteController potrà interagire solo con degli Amministratori.

AutenticazioneController assocerà, nel caso di autenticazione andata a buon fine, l'Utente alla sessione corrente offerta dal Broker.

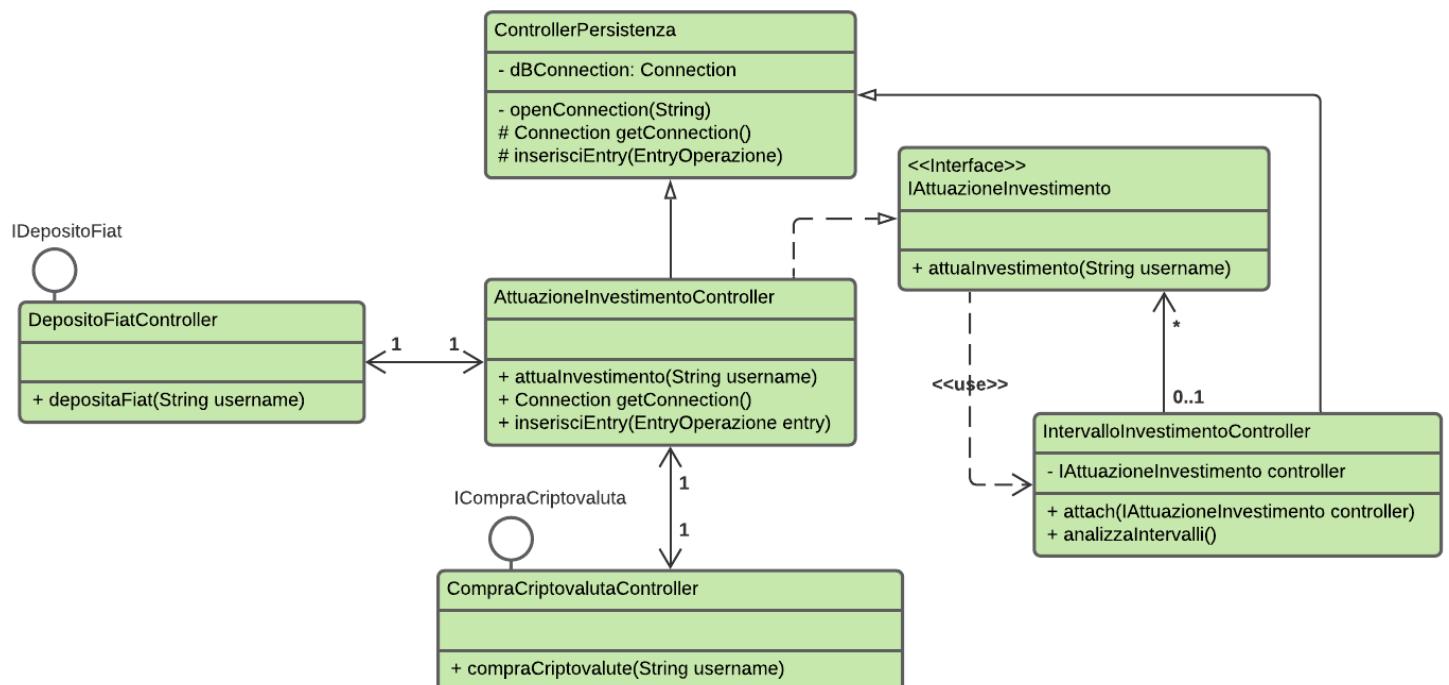
Per aumentare il livello di astrazione e l'estensibilità a future implementazioni della fase di registrazione, si è deciso di scomporre il processo su due controller differenti:

- *RegistrazioneController* effettua la *verificaDatiInseriti* e *registraUtente*, implementando l’interfaccia *IRegistrazione* che necessita della dipendenza con l’enumerativo *TipoDeposito*.
- *CodiceDiVerificaController* gestisce l’invio, alla mail specificata, del codice e la verifica dello stesso per completare il processo di registrazione.
Utilizzerà il metodo *inserisciEntry*, esposto da *RegistrazioneController*, per il salvataggio sui log delle operazioni svolte.

TipoDeposito è un enumerativo che rappresenta le diverse modalità di pagamento supportate dalla Piattaforma di Exchange per effettuare il deposito di valuta fiat.

RimuoviUtente effettuerà il processo di identificazione dell’Utente dalla Sessione, migliorando così la sicurezza e la privacy dei dati.

AttuazioneInvestimento



Si è deciso di scomporre il processo di investimento in fasi differenti, migliorando la modularità e l'estensibilità a future implementazioni, affidando compiti specifici a controller diversi:

- *DepositoFiatController* interagisce interfacciandosi alla Piattaforma di Exchange per depositare valuta fiat nel Portafoglio dell’Utente.
- *CompraCriptovalutaController*, in base alla DistribuzionePercentuale della StrategiaDCA scelta dall’Utente, effettua gli acquisti veri e propri di Criptovaluta creando il RiepilogoOrdine associato ad ogni acquisto.
- *AttuazioneInvestimentoController* espone i metodi per poter interagire con il DBMS. Il suo metodo *attualInvestimento* viene invocato allo scatenarsi dell’evento *IntervalloInvestimento*, realizzato mediante l’utilizzo di un pattern

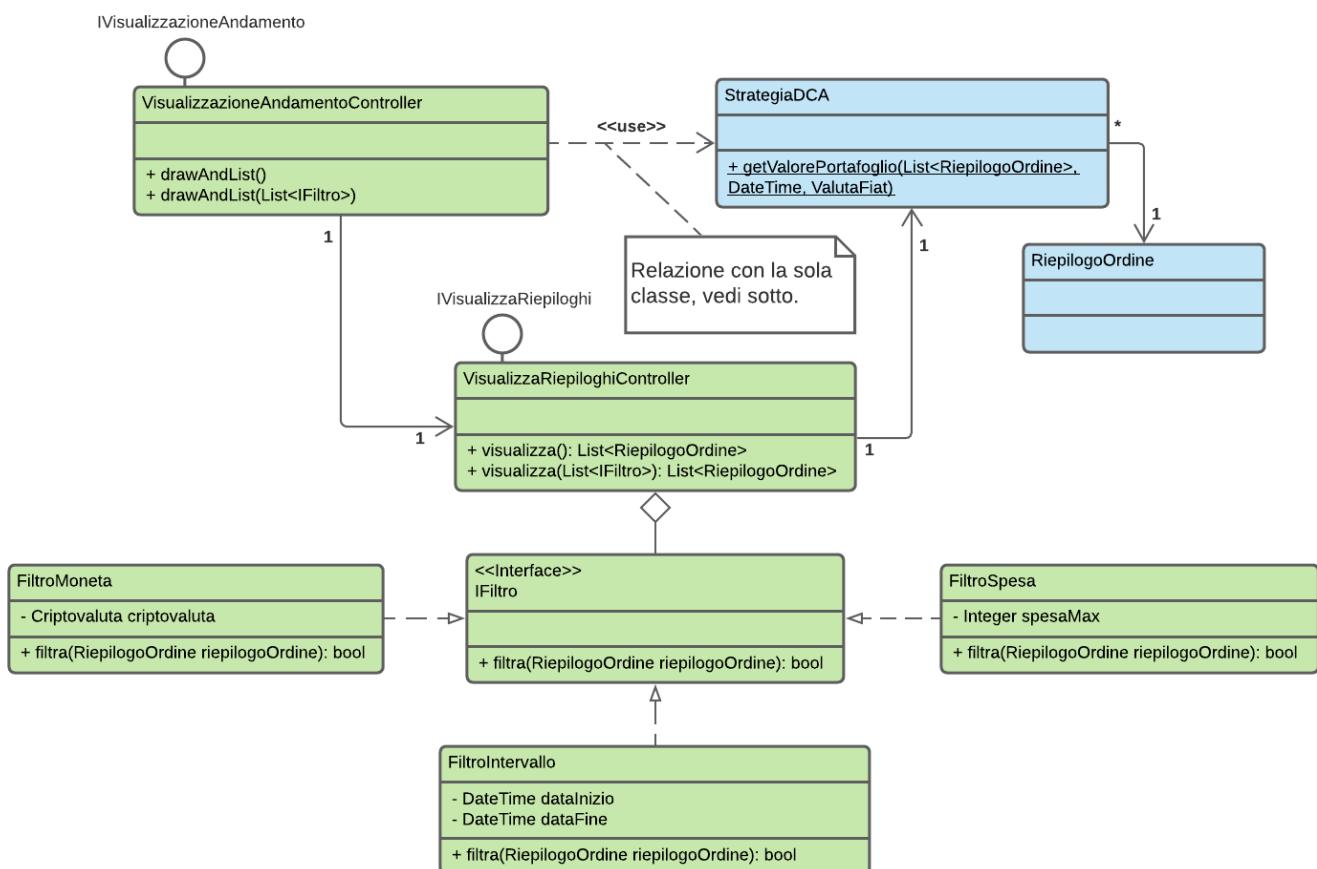
Observer basato su interfacce.

È stato scelto questo particolare approccio al pattern Observer per garantire maggiore astrazione e libertà rispetto alla scelta tecnologica.

È inoltre risultato errato utilizzare una lista di notifiche essendo controproducente effettuare l'attuazione dell'investimento per lo stesso Utente più volte contemporaneamente.

IntervalloInvestimentoController rappresenta il “worker” del pattern **Observer** che invocherà il metodo *attualInvestimento*, se nell'eseguire il metodo *analizzaIntervalli* identificherà un Utente il cui intervalloDlInvestimento (in giorni) è stato superato dall'ultimo investimento o nessun investimento è mai stato effettuato.

VisualizzazioneAndamento



Anche in questo caso si è scelto di scomporre i compiti per migliorare la modularità del progetto e facilitare future estensioni, in particolar modo scomponendo tra:

- **VisualizzaRiepiloghiController** che si avvale del pattern **Strategy** per restituire una lista di **RiepilogoOrdine** relativa all'Utente che li richiede.
- **VisualizzazioneAndamentoController**, utilizzando la lista di **RiepilogoOrdine** restituita da **VisualizzaRiepiloghiController**, produrrà un grafico

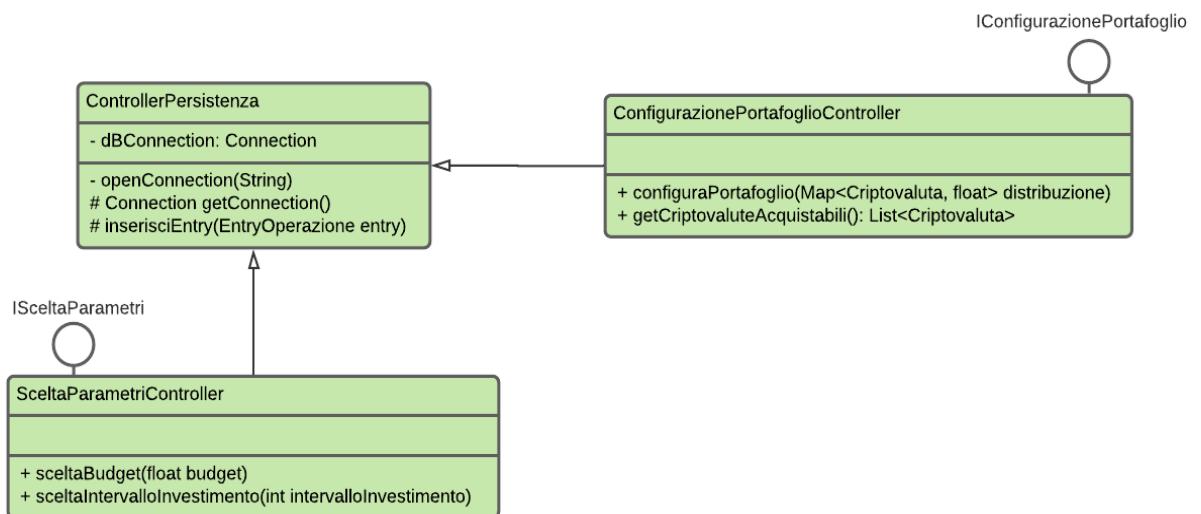
rappresentante l'andamento, nel tempo, del valore degli investimenti effettuati nel portafoglio dell'Utente grazie alla dipendenza con la classe `StrategiaDCA`. Da evidenziare come il suo collegamento con `StrategiaDCA` avvenga attraverso una relazione di uso, dato che necessita di utilizzare tutti e soli i servizi della classe (quindi il metodo statico `getValorePortafoglio`) e non necessita in alcun modo del referenziamento ad un'istanza della classe.

`IFiltro` è l'interfaccia usata per rappresentare il concetto di filtro nel pattern **Strategy**, utilizzando il metodo `filtra` asserisce se un certo `RiepilogoOrdine` rispetti o meno i criteri del filtro, al momento è possibile implementarlo mediante:

- `FiltroMoneta`
- `FiltroIntervallo`
- `FiltroSpesa`

Grazie all'utilizzo di questo pattern sarà inoltre possibile concatenare più criteri di filtraggio.

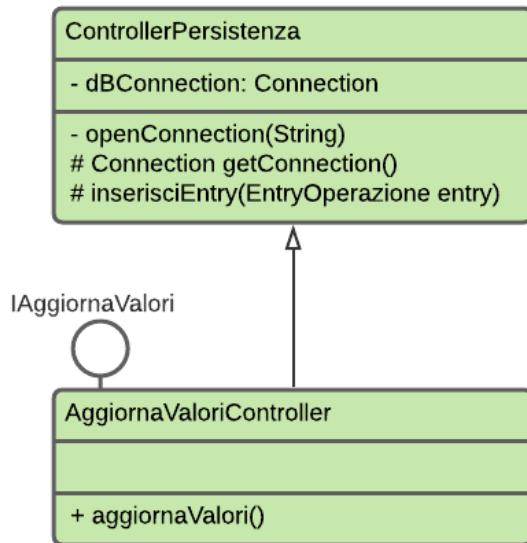
GestioneDCA



`SceitaParametriController` sarà utilizzato per la configurazione dei parametri di investimento dell'Utente.

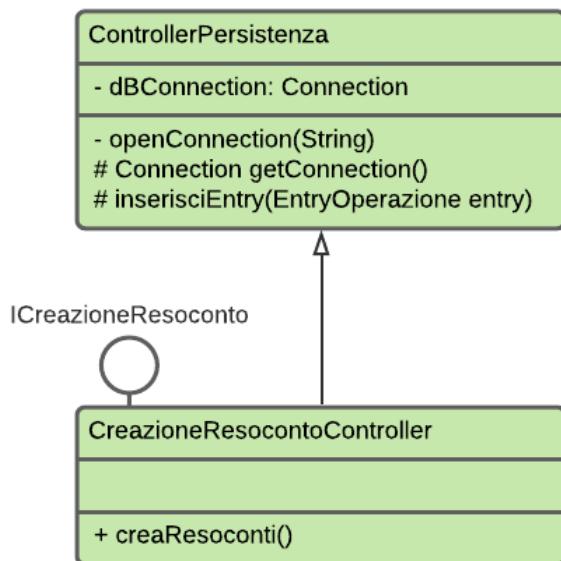
`ConfigurazionePortafoglioController` aggiorna la distribuzione percentuale dell'Utente ad ogni invocazione valida. Restituisce inoltre la lista delle Criptovalute acquistabili per la ValutaFiat di Riferimento dell'Utente che effettua la richiesta.

AggiornaValori



AggiornaValoriController effettua l'aggiornamento del valoreConversione tra le Criptovalute supportate e le ValuteFiat presenti.
A causa di limiti posti dalle API verso il sistema esterno, l'aggiornamento avverrà ogni 60 secondi.

CreazioneResoconto



CreazioneResocontoController alla fine di ogni mese produrrà un Resoconto Mensile per ogni Utente, inviandolo poi, come messaggio, all'indirizzo mail da lui specificato.

Log



LogController permetterà, attraverso i suoi metodi, di ottenere la lista di Entry offrendo anche la possibilità di applicare dei filtri.

Il metodo *analizzaOperazioni*, inoltre, consentirà di analizzare le EntryOperazione alla ricerca di eventuali anomalie.

Diagramma di dettaglio: Broker

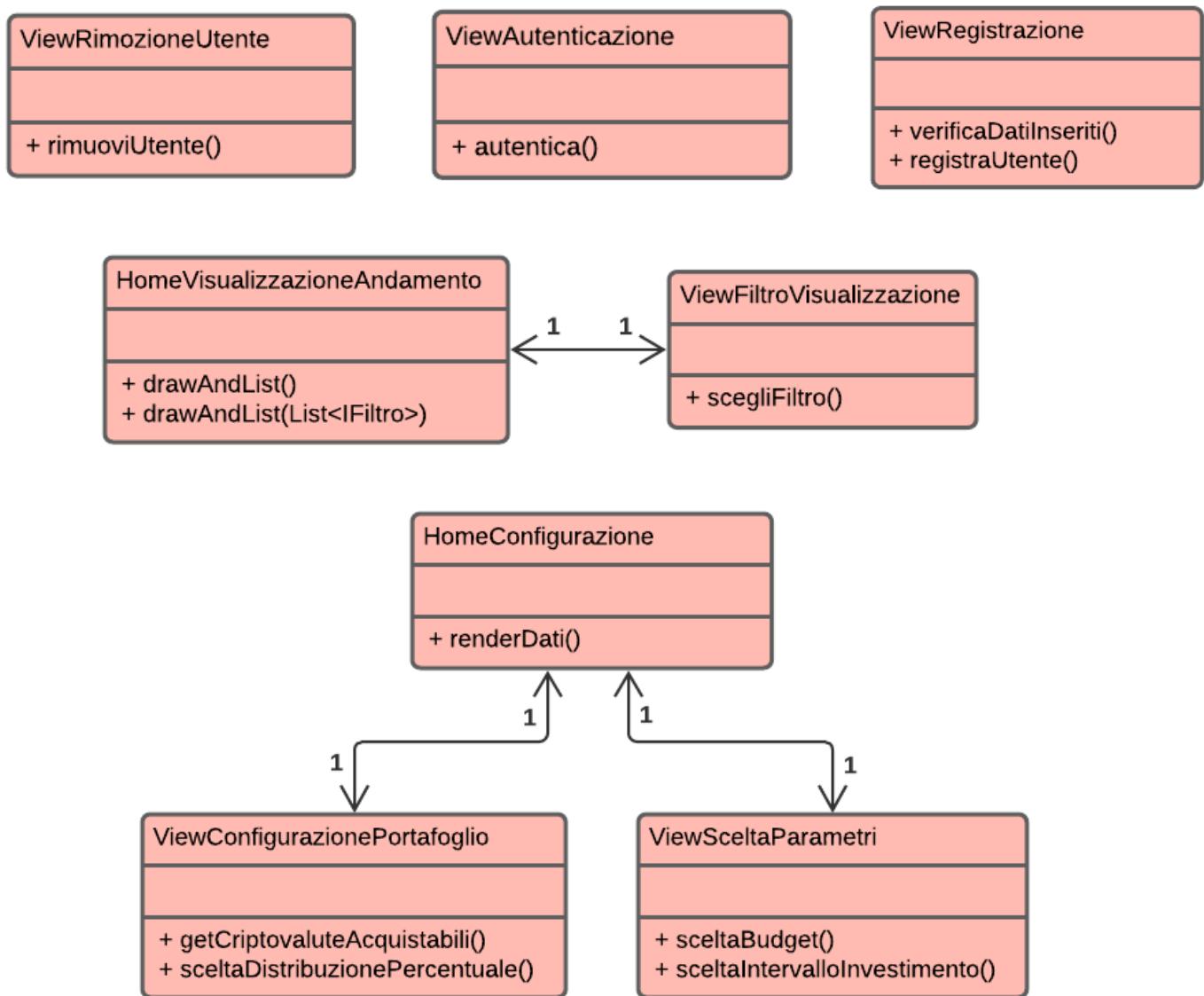
Avendo scelto di pubblicare la nostra applicazione sul web, il Broker sarà rappresentato da un web server. Si suppone che questo dia la possibilità di utilizzare una classe che rappresenti la sessione e mediante un'istanza permetta di impostare e recuperare dei valori da essa.

Sarà anche necessario che il Broker sappia gestire le richieste in entrata, inoltrandole al controller progettato per gestirle; allo stesso modo esso deve sapere inoltrare le risposte dei controller al cliente che ha richiesto il servizio.

Diagramma di dettaglio: Client

Utente

Essendo l'applicazione basata sul web, i client non necessitano di una logica applicativa, ma semplicemente risponderanno alle interazioni con l'Utente trasmettendo le richieste al server.



Si è deciso di visualizzare la previsione della spesa, rispetto ai Parametri di Investimento, direttamente dentro la **HomeConfigurazione**. Essa inoltre sarà aggiornata all'invocazione di `renderDati`, da parte di **ViewConfigurazionePortafoglio** o **ViewSceltaParametri**, ogni qualvolta vengano modificati i Parametri di Investimento e/o la Distribuzione Percentuale dall'Utente dalle stesse.

La **HomeVisualizzazioneAndamento** mostra i Riepiloghi dell'Ordine prodotti dagli investimenti dell'utente con una rappresentazione grafica nel tempo. Viene

aggiornata ad ogni invocazione di drawAndList, con la possibilità di applicare o meno dei filtri da ViewFiltroVisualizzazione.

Interfaccia Registrazione

È possibile inserire il codice di verifica solo in seguito alla convalida e verifica dei dati inseriti da parte del server.

Registrazione

Inserisci le informazioni richieste

Username:

Email:

Password:

ApiKey:

ApiSecret:

Valuta Fiat:

Modo con cui effettuare i depositi:

Richiedi Codice di Verifica

Codice di Verifica:

Registrati

Registrazione

Inserisci le informazioni richieste

Username:

Email:

Password:

ApiKey:

ApiSecret:

Valuta Fiat:

Modo con cui effettuare i depositi:

Richiedi Codice di Verifica

Codice di Verifica:

Registrati

Interfaccia Login

Login

Username:

Password:

Esegui il login

Interfaccia RimozioneAccount



Interfaccia VisualizzazioneAndamento

Visualizzazione Andamento



Amministratore

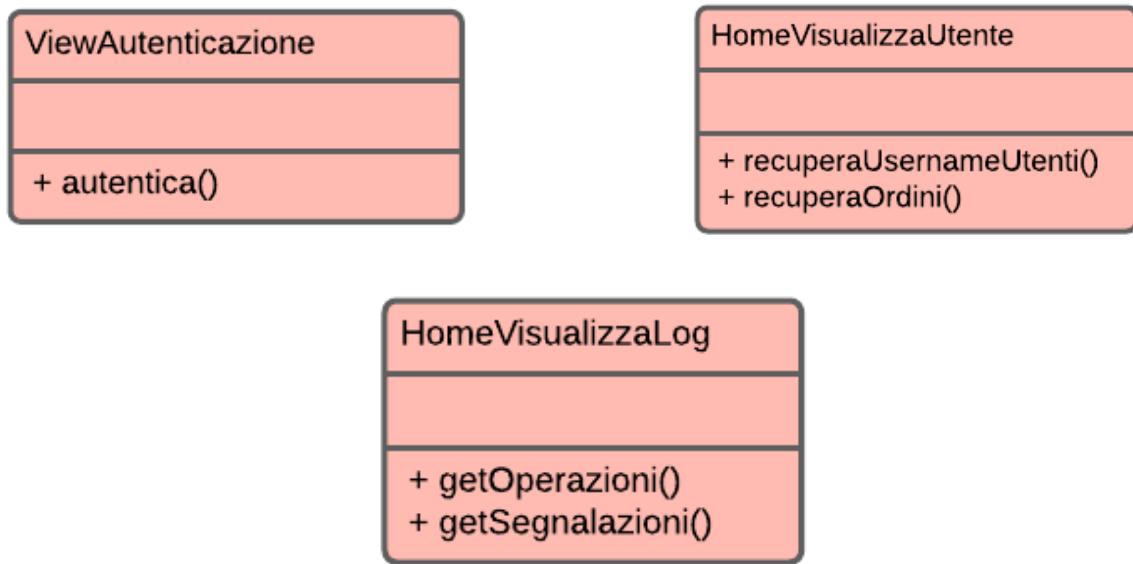
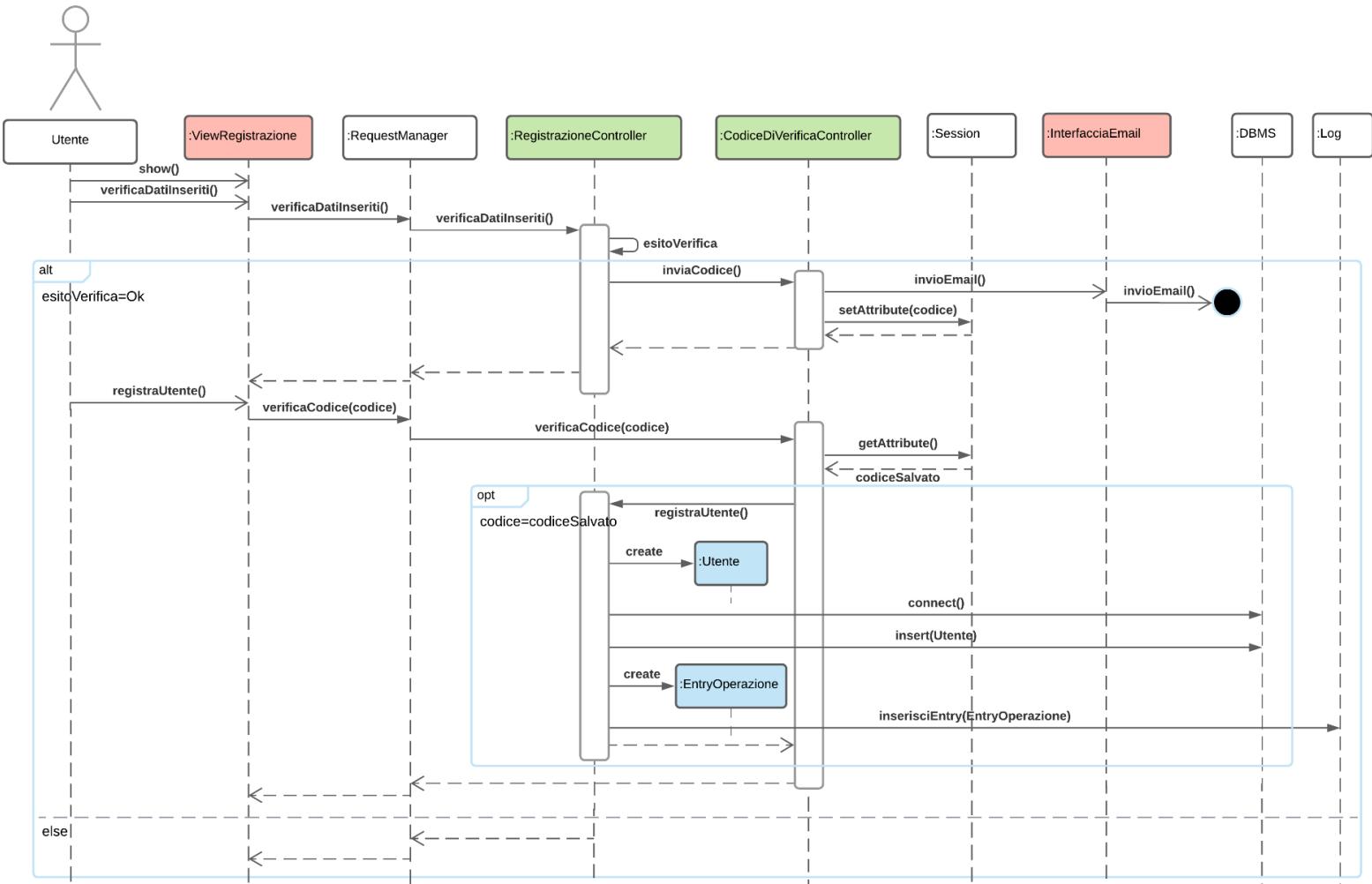


Diagramma di dettaglio: Interazione

Registrazione



Per migliorare la leggibilità del diagramma si è omesso il salvataggio in sessione dei dati passati dall'Utente con la *verificaDatiInseriti*.

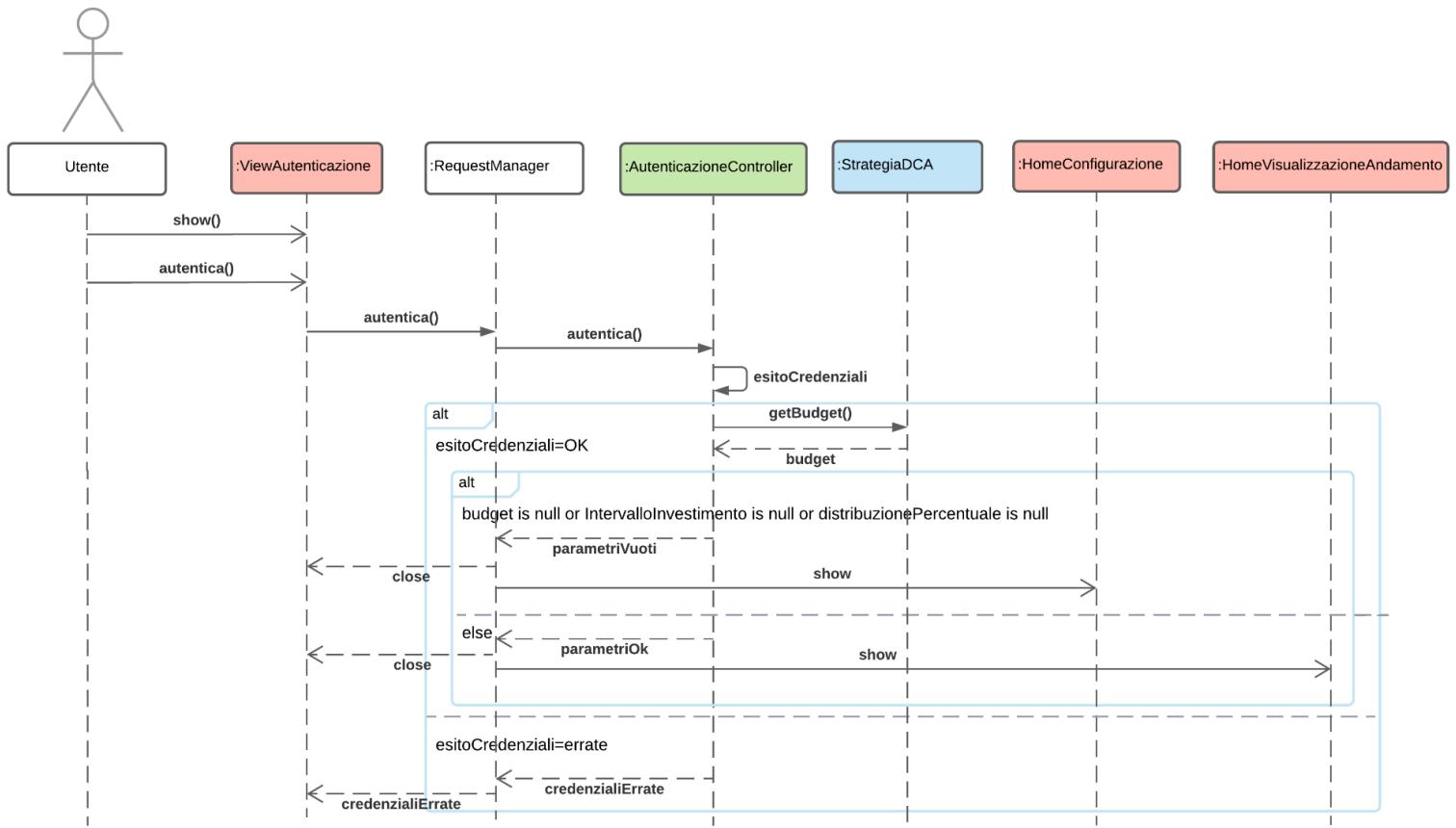
Inoltre in fase di *registraUtente* verranno recuperati dalla sessione tali dati, dopo la verifica del codice, per essere salvati poi sul DBMS.

Per garantire sicurezza, i dati critici saranno cifrati prima di essere salvati in sessione.

Per motivi di spazio e leggibilità del diagramma sono state omesse le fasi di creazione ed inserimento nei log delle operazioni relative alla fase di *invioEmail*.

Non si evidenzia in questo diagramma la gestione di errori o eccezioni nella creazione di istanze del modello del dominio e interazioni con la persistenza.

Autenticazione



L'*esitoCredenziali* viene calcolato da *AutenticazioneController* in seguito ad un'interazione con il database (omessa per migliorare la leggibilità), verificando le credenziali passate dall'Utente.

Saranno salvate nei log tutte le operazioni relative ai tentativi di autenticazione effettuati.

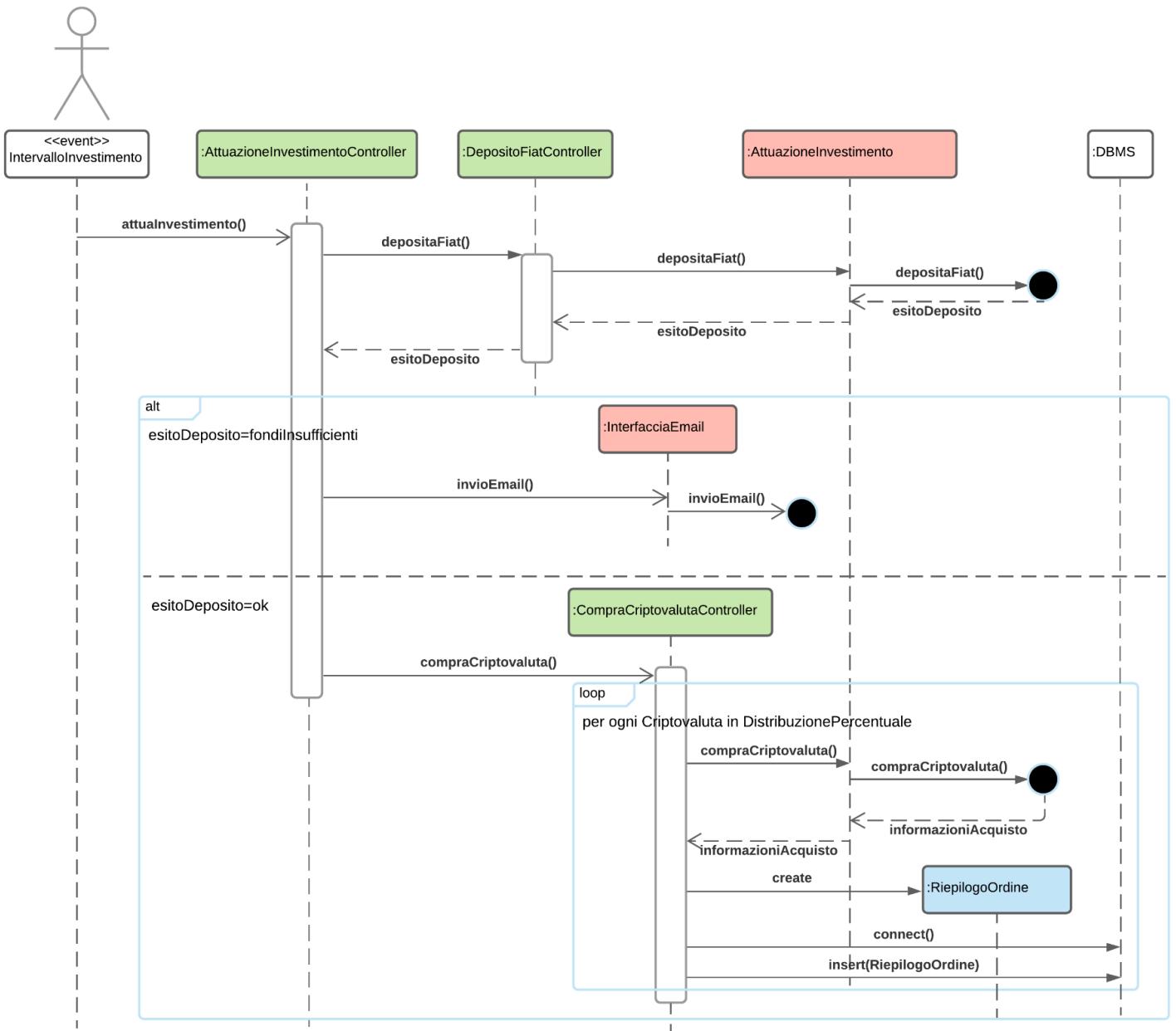
Sarà inoltre necessario effettuare il salvataggio in sessione di un'istanza relativa all'Utente per un'autenticazione andata a buon fine.

La *StrategiaDCA* sarà ricavata direttamente tramite il DBMS grazie all'associazione con l'Utente appena autenticato.

Allo stesso modo in cui viene recuperato e verificato il Budget della *StrategiaDCA* dell'Utente, *AutenticazioneController* recupera e verifica se l'Intervallo di Investimento e la Distribuzione Percentuale sono impostati.

Per migliorare la leggibilità del diagramma, in particolar modo all'interno dei componenti UML "CombinedFragment", sono state omesse le barre di attivazione di tutti gli elementi.

AttuazioneInvestimento



Per migliorare la leggibilità sono state omesse tutte le scritture di log relativi alle operazioni di invio dell'email e dell'acquisto delle criptovalute.

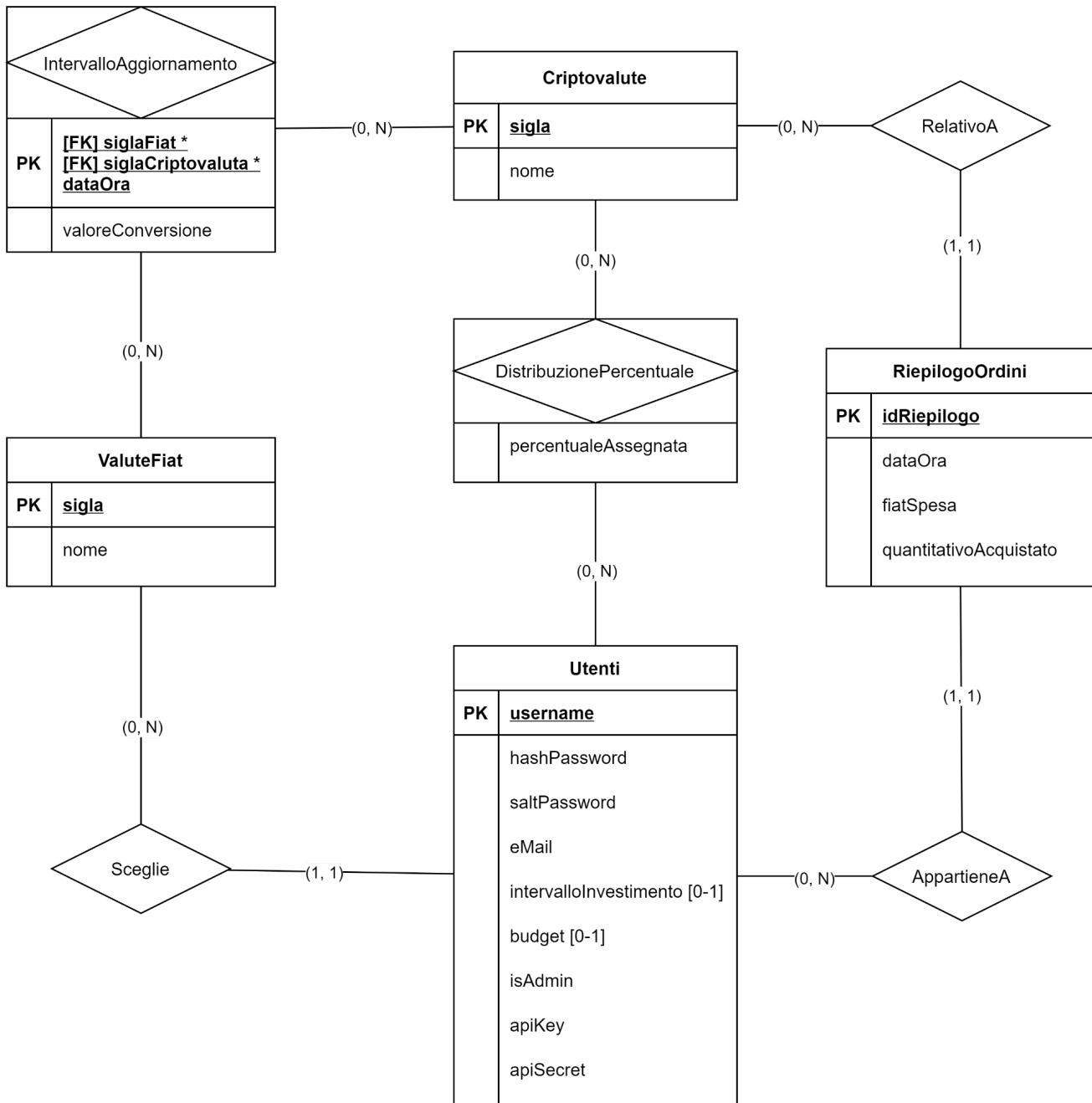
I dati per connettersi al portafoglio dell'Utente nella Piattaforma di Exchange verranno recuperati dal DBMS, previa decifrazione.

Diagramma di dettaglio: Comportamento

Come per la fase di analisi, si omettono i diagrammi di stato/attività in quanto ritenuti non necessari.

Progettazione della persistenza

Diagramma ER



La presenza di un ciclo tra Criptovalute, Utenti e RiepilogoOrdini implica un vincolo su RiepilogoOrdini, in quanto un RiepilogoOrdine per un Utente può essere generato solamente in relazione ad una Criptovaluta presente nella DistribuzionePercentuale di quello stesso Utente.

L'Utente deve avere una ValutaFiat per cui le Criptovalute nella sua Distribuzione Percentuale sono associate alla ValutaFiat stessa; questo vincolo è già intrinseco nel

sistema non essendo possibile per un Utente modificare la sua ValutaFiat di Riferimento dopo aver effettuato la fase di registrazione.

Infine è anche deducibile come la semantica delle relazioni tra ValuteFiat con Utenti e con Criptovalute sia differente; ciò è stato confermato da test successivi effettuati nella progettazione del collaudo.

Formato del File Log

- Formato dei Log delle operazioni:
Data e ora - Tipo di operazione - Messaggio
- Formato dei Log delle anomalie:
Data e ora - Messaggio

Progettazione del collaudo

Di seguito alcuni dei test che verificano il corretto funzionamento delle classi del modello del dominio:

```
class TestProgettazione
{
    private StrategiaDCA strategiaDCA;
    private Criptovaluta criptovaluta;
    private ValutaFiat valutaFiat;

    @BeforeEach
    void setup()
    {
        /* Dichiarazione e creazione StrategiaDCA e suoi attributi */
        strategiaDCA = new StrategiaDCA();
        Map<Criptovaluta, Float> distribuzionePercentuale = new HashMap<>();

        /* Dichiarazione e creazione Criptovaluta e strutture per i referenziamenti */
        criptovaluta = new Criptovaluta();
        // Dichiarazione e creazione mappa di mappe che associa Criptovaluta a ValutaFiat
        Map<ValutaFiat, Float> valoriConversione = new HashMap<>();
        Map<LocalDateTime, Map<ValutaFiat, Float>> intervalliAggiornamento = new HashMap<>();

        /* Dichiarazione e creazione ValutaFiat e lista di Criptovalute disponibili*/
        valutaFiat = new ValutaFiat();
        List<Criptovaluta> criptovaluteDisponibili = new ArrayList<>();

        /* Inizializzazione dei valori degli attributi di strategiaDCA */
        strategiaDCA.setBudget(100f);
        strategiaDCA.setIntervalloInvestimento(30);

        /* Inizializzazione valori di criptovaluta */
        criptovaluta.setNome("Ethereum");
        criptovaluta.setSigla("ETH");

        /* Inizializzazione valori di valutaFiat */
        valutaFiat.setNome("Euro");
        valutaFiat.setSigla("EUR");

        /* Inizializzazione di un valore nella mappa di mappe in Criptovaluta */
        valoriConversione.put(valutaFiat, 2018.23f);
        intervalliAggiornamento.put(LocalDateTime.of(2021, 05, 28, 17, 47, 13),
        valoriConversione);
        criptovaluta.setIntervalliAggiornamento(intervalliAggiornamento);

        /* Inizializzazione Lista di Criptovalute disponibili nella valuta fiat */
        criptovaluteDisponibili.add(criptovaluta);
        valutaFiat.setCriptovaluteAssociate(criptovaluteDisponibili);
    }
}
```

```

/* Inizializzazione di distribuzionePercentuale e inserimento strategiaDCA */
distribuzionePercentuale.put(criptovaluta, 100f);
strategiaDCA.setDistribuzionePercentuale(distribuzionePercentuale);
}

@Test
void testStrategiaDCA()
{
    assertTrue(strategiaDCA instanceof StrategiaDCA);
    assertEquals(strategiaDCA.getBudget(), 100f);
    assertEquals(strategiaDCA.getIntervalloInvestimento(), 30);
    assertEquals(strategiaDCA.getDistribuzionePercentuale().get(criptovaluta), 100f);
}

@Test
void testCriptovaluta() {
    assertTrue(criptovaluta instanceof Criptovaluta);
    assertEquals(criptovaluta.getNome(), "Ethereum");
    assertEquals(criptovaluta.getSigla(), "ETH");
    assertEquals(criptovaluta.getIntervalliAggiornamento().get(LocalDateTime.of(2021, 05, 28, 17, 47, 13)).get(valutaFiat), 2018.23f);
    assertEquals(criptovaluta.getValore(valutaFiat, LocalDateTime.of(2021, 05, 28, 17, 47, 13)), 2018.23f);
}

@Test
void testValutaFiat() {
    assertTrue(valutaFiat instanceof ValutaFiat);
    assertEquals(valutaFiat.getNome(), "Euro");
    assertEquals(valutaFiat.getSigla(), "EUR");
    assertEquals(valutaFiat.getCriptovaluteAssociate().get(0).getNome(), "Ethereum");
}
}

```

Sono state inoltre effettuate delle verifiche sulla consistenza ed effettiva differenza di semantica delle relazioni del diagramma ER costruendo un database di prova per evidenziare il corretto funzionamento dello stesso, mediante l'esecuzione di query SQL:

```

-- Visualizzazione della percentualeAssegnata ad ogni Criptovalute da un Utente
SELECT
    Criptovalute.sigla,
    DistribuzionePercentuale.percentualeAssegnata
FROM
    Utenti

```

```

    INNER JOIN DistribuzionePercentuale ON Utenti.username =
        DistribuzionePercentuale.username
    INNER JOIN Criptovalute ON Criptovalute.sigla =
        DistribuzionePercentuale.siglaCriptovaluta
WHERE
    Utenti.username = "MasterDCA";

```

```

-- Visualizzazione del valore del portafoglio di un Utente ad una certa data per la
sua valutaFiatRiferimento
SELECT
    sum(TotaleValoreCriptoInValutaFiat)
FROM
    (SELECT
        (sum(quantitativoAcquistato) *
        (SELECT
            valoreConversione
        FROM
            IntervalloAggiornamento
        WHERE
            IntervalloAggiornamento.siglaCriptovaluta = R.siglaCriptovaluta AND
            IntervalloAggiornamento.siglaFiat = V.sigla
        ORDER BY
            abs(strftime('%s', IntervalloAggiornamento.dataOra) -
            strftime('%s', datetime())) ASC
        LIMIT 1)
    ) as 'TotaleValoreCriptoInValutaFiat'
FROM
    RiepilogoOrdini as R
    INNER JOIN Utenti as U ON U.username = R.username
    INNER JOIN ValuteFiat as V ON V.sigla = U.valutaFiatRiferimento
WHERE
    U.username = "MasterDCA" AND
    date(dataOra) <= date('2021-05-26')
GROUP BY
    R.siglaCriptovaluta
);

```

Entrambe vengono completate con successo senza causare errori alle dipendenze:

```

Esecuzione completata senza errori.
Risultato: 2 righe ritornate in 18ms

```

Progettazione del deployment

Deployment per la sicurezza

Per quanto riguarda i server, questi vanno installati su delle macchine poste in una rete privata e le comunicazioni all'interno di tale rete devono essere cifrate, mediante l'uso di VPN se collocate in zone fisiche differenti.

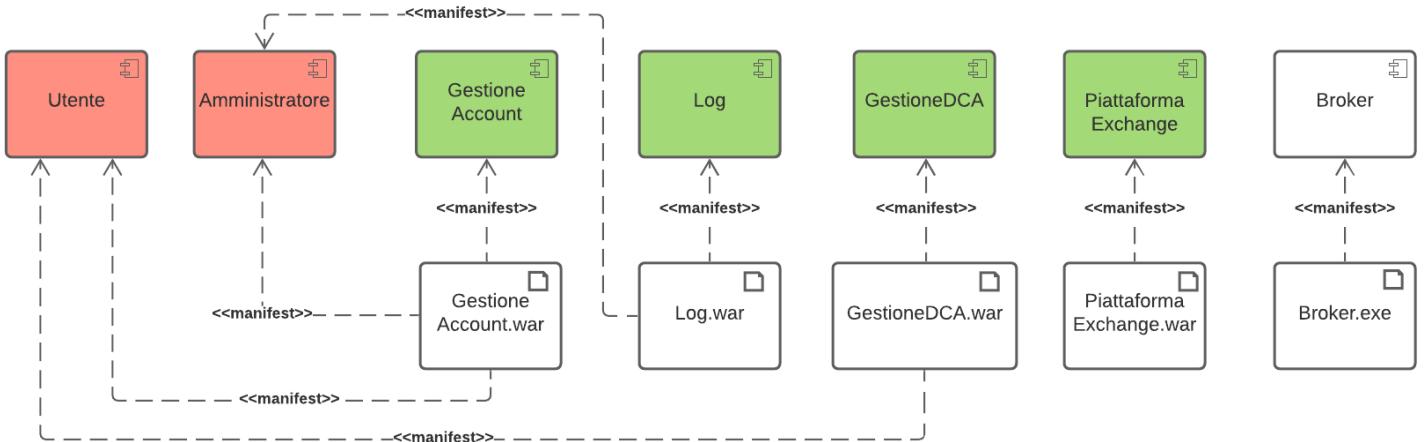
Tutte le comunicazioni dirette ai server devono essere obbligatoriamente filtrate dal Broker e non deve essere possibile in alcun modo raggiungerli in maniera diversa dall'esterno.

Per rispettare il vincolo del minimo privilegio, si è deciso inoltre che, superata la fase di registrazione, l'account non debba disporre dei privilegi di Amministratore.

Essendo il sistema dipendente da tecnologie basate sul web l'aggiornamento sarà effettuato in automatico alla modifica dei client, dato che questi risiedono sui server e sono offerti ai browser dai server stessi.

Deployment del sistema

Di seguito il diagramma relativo agli artefatti del sistema:



Di seguito il diagramma relativo al deployment type-level:

